

Data Protection in Peru: Overview

by Oscar Montezuma and Fiorella Colonna, Niubox, with Practical Law Data Privacy Advisor

Status: **Law stated as of 01-Jun-2023** | Jurisdiction: **Peru**

This document is published by Practical Law and can be found at: uk.practicallaw.tr.com/w-012-4508
Request a free trial and demonstration at: uk.practicallaw.tr.com/about/freetrial

A Q&A guide to data protection in Peru.

This Q&A guide gives a high-level overview of the data protection laws, regulations, and principles in Peru, including the main obligations and processing requirements for data controllers, data processors, and other third parties. It also covers data subject rights, the supervisory authority's enforcement powers, and potential sanctions and remedies. It briefly covers rules applicable to cookies and spam.

To compare answers across multiple jurisdictions, visit the Data Protection [Country Q&A Tool](#).

Regulation

Legislation

1. What national laws regulate the collection, use, and disclosure of personal data?

Data Protection Law

In Peru, the following laws regulate the collection, use, and disclosure of personal data:

- [Personal Data Protection Law](#) (Law No. 29733), which [Legislative Decree 1353](#) amended (together Amended PDPL) (both in Spanish).
- [Personal Data Protection Regulation](#), which Supreme Decree No. 003-2013-JUS approved (in Spanish).
- [Personal Data Protection Legislative Decree Regulation \(Supreme Decree No. 019-2017-JUS\)](#) (PDP Legislative Decree Regulation) (in Spanish), which governs the National Authority for Personal Data Protection (NAPDP), Peru's data protection authority, and details sanctions under the Amended PDP Law and PDP Regulation.
- [Peruvian Political Constitution](#) (Constitution), which gives every person the right or the assurance that information services, whether computerized, public, or private, will not provide information affecting personal and family privacy (Article 2(6), Constitution).

Other Relevant Laws

Peru has several other relevant laws that regulate the collection, use, and disclosure of personal data, including:

- The [National Authority for Personal Data Protection Directive on Security of Information No. 019-2013-JUS/DGPDP](#) (in Spanish), which establishes security standards for storing personal data (see Question 15).
- The [Anti-Spam Law No. 28493](#) (in Spanish), which regulates unsolicited commercial emails (see Question 18).
- The [Consumer Protection and Defense Code Law No. 29571](#) (in Spanish), which prohibits commercial contact to consumers through instant messaging, emails, or calls without consent in Article 58.
- The [Private Credit Reporting Law No. 27489](#) (in Spanish), which regulates the use of data to evaluate private credit reports.
- The following laws, which protect the secrecy of telecommunications and regulate interception, disclosure, and access to personal data:
 - the [Telecommunications Act](#) (in Spanish), which [Supreme Decree No. 013-2018-MTC](#), [Supreme Decree No. 015-2019-MTC](#), [Supreme Decree No. 018-2021-MTC](#), amended; and
 - [Resolution No. 111-2009-MTC](#) (in Spanish).
- The [General Law of the Financial and Insurance System and Organic Law of the Superintendence of](#)

Banking and Insurance, Law No. 26702 (in Spanish) which Law No. 31143 and Legislative Decree No. 1531 amended, which sets the general legal framework to protect clients' financial information. In addition, Circular No. G-140-2009-SBS, which Circular No. G-193-2017 (both in Spanish) modified, provides guidelines on information security management for banking and financial institutions.

- [Directorial Resolution No. 02-2020-JUS/DGTAIPD](#) (in Spanish), which regulates video surveillance.
- [Administrative Directive No. 294-MINSA/2020/OGTI](#) (in Spanish), which provides guidelines on the proper use of personal data in healthcare situations under the Amended PDPL.

This Q&A focuses on the Amended PDPL and its regulations. Other relevant laws are generally outside its scope.

Scope

2. To whom do the laws apply?

The [Personal Data Protection Law](#) (Law No. 29733), which [Legislative Decree 1353](#) amended (together Amended PDPL), and [Personal Data Protection Regulation](#) (PDP Regulation) (all in Spanish) apply to any public or private person or legal entity processing personal data.

The Amended PDPL includes the following definitions:

- **Holder of personal data**, known in other jurisdictions as a data subject, means any natural person to whom the personal data belongs (Article 2(16), Amended PDPL).
- **Holder of the personal data bank**, known in other jurisdictions as a data controller, means anyone who determines the purpose and content of a personal data bank, its processing, and security measures, including any:
 - natural person;
 - legal entity under private law; or
 - public entity.

(Article 2(17), Amended PDPL; for more on personal data banks, see Question 3; for more on the main obligations of holders of personal data banks, see Question 8.)

- **Manager of the personal data bank**, known in other jurisdictions as a data processor, means any natural person or legal entity under private law, or any public entity that carries out the processing of personal data, by itself or jointly with others, on the holder of a

personal data bank's behalf by virtue of an agreement that binds it to the same liabilities and delimits the scope of its actions (Article 2(7), Amended PDPL; Article 2(11), (14), PDP Regulation; for more on working with managers of personal data banks, see Question 17).

- **Issuer and exporter of personal data**, which are holders of a personal data bank that transfer data to another country (Article 2(9), PDP Regulation; for more on exporting personal data, see Question 20).
- **Receiver or importer of personal data**, which is any natural or legal person that receives personal data from abroad (Article 2(11), PDP Regulation; for more on receiving personal data from outside of Peru, see Question 20).
- **Third party**, which is anyone other than the holder of personal data, holder of a personal data bank, or manager of a personal data bank, who processes personal data (Article 2(15), PDP Regulation).

For more on:

- The definition of personal data, see Question 3.
- The Amended PDPL's and PDP Regulation's regulated activities, see Question 4.

3. What personal data does the law regulate?

The [Personal Data Protection Law](#) (Law No. 29733), which [Legislative Decree 1353](#) amended (together Amended PDPL), and [Personal Data Protection Regulation](#) (PDP Regulation) (all in Spanish) apply to personal data, meaning:

- Any information related to an identified or identifiable natural person using reasonable means.
- Any numerical, alphabetical, graphic, photographic, and acoustic information, about personal habits, or any other type concerning a natural person that identifies the person or makes the person identifiable through reasonable means.

(Article 2(4), Amended PDPL; Article 2(4), PDP Regulation.)

The definition may cover anonymous, individualized personal data, like cookie identifiers, that organizations may use to create individualized profiles, if the personal data relates to an identified or identifiable natural person. Holders of personal data banks, which are similar to data controllers in other jurisdictions, that apply an anonymization or dissociation procedure may not need to obtain consent from holders of personal data, who are similar to data subjects in other jurisdictions (Article 14(8), Amended PDPL). The Amended PDPL defines:

- **Anonymization as an irreversible** procedure that allows personal data processing that:
 - prevents identification; or
 - does not make the holder of the personal data identifiable.
- **Disassociation as a reversible** procedure that allows personal data processing that:
 - prevents identification; or
 - does not make the holder of the personal data identifiable.

(Article 2(12), (13), Amended PDPL; for more on when consent is necessary and the exceptions to consent, see Question 9 and Question 10.)

The Amended PDPL and PDP regulation also regulate personal data banks, defined as an organized group of non-automated and automated personal data, regardless of its creation, formation, storage, organization, and access, be it physical, magnetic, digital, optical, or other (Article 2(1), Amended PDPL; Article 2(1), PDP Regulation).

The Amended PDPL and PDP Regulation also apply to sensitive data, meaning:

- Biometric data that by itself can identify the owner.
- Personal data referring to:
 - racial and ethnic origin;
 - personal income;
 - opinions or political, philosophical, or moral beliefs;
 - union membership;
 - physical or mental health or sexual life;
 - physical, moral, or emotional characteristics;
 - facts or circumstances of emotional or family life; or
 - personal habits that correspond to the most intimate sphere.
- Analogous information that affects a person's privacy.

(Article 2(5), Amended PDPL; Article 2(6), PDP Regulation.)

For more on:

- The Amended PDPL's and PDP Regulation's regulated activities, see Question 4.
- Processing sensitive data in Peru, see Question 11.

4. What acts are regulated?

The [Personal Data Protection Law](#) (Law No. 29733), which [Legislative Decree 1353](#) amended (together

Amended PDPL) and [Personal Data Protection Regulation](#) (PDP Regulation) (all in Spanish) apply to personal data processing (Article 3, Amended PDPL; Article 3, PDP Regulation; for more information about exemptions, see Question 6).

The Amended PDPL defines processing as any operation or technical procedure, automated or not, that allows:

- Compiling, registration, and organization.
- Storage, conservation, and preparation.
- Modification, extraction, and consultation.
- Utilization, blockage, and suppression.
- Communication by transfer or distribution.
- Access, correlation, or interconnection of the personal data.

(Article 2(2), (3), and (19), Amended PDPL.)

For more on anonymization or dissociation procedures, see Question 3. For more on processing sensitive data, see Question 11.

5. What is the jurisdictional scope of the rules?

The [Personal Data Protection Law](#) (Law No. 29733), which [Legislative Decree 1353](#) amended (together Amended PDPL), and [Personal Data Protection Regulation](#) (PDP Regulation) (all in Spanish) apply to personal data processing carried out by:

- A Peru-established holder of a personal data bank, which other jurisdictions commonly refer to as a data controller, or a manager of a personal data bank, which other jurisdictions commonly refer to as a data processor.
- A data processor not established in Peru acting on behalf of a Peru-based holder of a personal data bank or a Peru-based manager of a personal data bank.
- A holder or manager of a personal data bank not established in Peru, when Peruvian law applies by contract or international law.
- A holder or manager of personal data bank based outside of Peru who uses means located in Peru, unless the means are only for transit purposes. In this case, the holder of a personal data bank must appoint a representative in Peru or implement adequate mechanisms to comply with Peruvian law. In all other cases, when a holder of a personal data bank is not established in Peru, Peru does not require it to appoint a local representative to address concerns from holders of personal data or the NAPDP.

(Article 3, Amended PDPL; Article 5, PDP Regulation.)

6. What are the main exemptions (if any)?

The [Personal Data Protection Law](#) (Law No. 29733), which [Legislative Decree 1353](#) amended (together Amended PDPL), and [Personal Data Protection Regulation](#) (PDP Regulation) (all in Spanish) do not apply to personal data included in:

- A personal data bank created exclusively for private or domestic purposes (for more on personal data banks, see Question 3).
- A public data bank if the personal data processing is necessary:
 - to comply with the legal responsibilities of public entities; and
 - for national defense, public safety, or criminal investigation purposes.

(Article 3, Amended PDPL; Article 4, PDP Regulation.)

Notification

7. Is notification or registration with a supervisory authority required before processing data?

The [Personal Data Protection Law](#) (Law No. 29733), which [Legislative Decree 1353](#) amended (together Amended PDPL), and [Personal Data Protection Regulation](#) (PDP Regulation) (all in Spanish) require holders of personal data banks, which other jurisdictions commonly refer to as data controllers, to register personal data banks with the NAPDP before processing personal data (Article 28(8), Amended PDPL; Article 78, PDP Regulation). For the NAPDP's contact details, see Box, Regulator Details.

Holders of personal data banks must fill out a form and provide the following information:

- The name and location of the personal data bank.
- The holder of a personal data bank's identity and where appropriate, the identification of the person processing personal data on the personal data bank holder.
- The personal data bank's purpose and use.
- The type of personal data the data bank includes.
- The security measures the data bank implements.
- Procurement procedures and the system of processing personal data.
- Any third-party recipients of personal data transfers.

(Article 79, PDP Regulation.)

Holders of personal data banks must update the registry to reflect any changes. The forms are available on the Government [website](#).

For more:

- Guidance on registration from the NAPDP, see [National Registry of Protection of Personal Data](#) (in Spanish).
- Information on individual notification requirements, see Question 12.

Main Data Protection Rules and Principles

Main Obligations and Processing Requirements

8. What are the main obligations imposed on data controllers to ensure data is processed properly?

Under the [Personal Data Protection Law](#) (Law No. 29733), which [Legislative Decree 1353](#) amended (together Amended PDPL), and [Personal Data Protection Regulation](#) (PDP Regulation) (all in Spanish), holders of personal data banks, which other jurisdictions commonly refer to as data controllers, must comply with the following obligations:

- Process personal data only when the holder of personal data, which other jurisdictions commonly refer to as data subjects, provides prior, free, express, unequivocal, and informed consent, unless the law provides otherwise (for more on consent, see Question 9).
- Not use fraudulent, unfair, or unlawful means to collect personal data.
- Ensure that personal data processing is adequate, relevant, and not excessive for the collection's purposes. Other jurisdictions commonly refer to this as data minimization.
- Collect personal data only for specified, explicit, and legitimate purposes and not process personal data in a manner that is incompatible with those purposes, unless the personal data undergoes an anonymization or dissociation process. Other jurisdictions commonly refer to this as purpose limitation.
- Store personal data in a manner that allows holders of personal data to enforce their rights.
- Delete or correct personal data on knowledge of its inaccuracy or incompleteness.
- Provide the NAPDP with access to the personal data bank on request to exercise its functions or for administrative proceedings.

- Register personal data banks with the NAPDP before processing personal data (for more on registration requirements, see Question 7).
- Work only with managers of personal databanks, which other jurisdictions commonly refer to as data processors, if they guarantee compliance with the law. In certain cases, an agreement or contract with the manager of personal data banks is necessary, such as if the processing or treatment involves human intervention. The Amended PDPL and the PDP Regulation do not specify whether the agreement has to be in writing, but a written agreement is highly recommended due to enforcement actions. For more on working with third parties, see Question 17.

(Articles 28 and 29, Amended PDPL; Articles 30, 33, 34, 37, 38 and 78, PDP Regulation.)

Personal data processing must respect the holder of personal data's fundamental rights and the rights that Peruvian law grant to them (for more on these rights, see Question 12 and Question 13).

The holder of a personal data bank, the manager of a personal data bank, and any other entity processing personal data must keep the personal data confidential, unless exceptions apply. Confidentiality must be maintained even after the termination of the relationship between the holder of personal data and the holder of a personal data bank (Article 17, Amended PDPL).

Peru's data protection laws do not include an obligation to appoint a designated individual to oversee the organization's compliance to the law. However, a holder of a personal data bank not based in Peru, but who uses means located in Peru not solely for transfer purposes, may have obligations to appoint a local representative in Peru (see Question 5).

For more information on:

- The Amended PDPL's and PDP Regulation's regulated acts, see Question 4.
- Processing sensitive data, see Question 11.

9. Is the consent of data subjects required before processing personal data?

The [Personal Data Protection Law](#) (Law No. 29733), which [Legislative Decree 1353](#) amended (together Amended PDPL), and [Personal Data Protection Regulation](#) (all in Spanish) require the consent of the holder of personal data before processing personal data unless an exception applies (Article 13(5), Amended PDPL; Articles 7 and 12, PDP Regulation). Other jurisdictions commonly refer to holders of personal data as data subjects. For more on data processing without consent, see Question 10.

Valid Consent Elements

The Amended PDPL and PDP Regulation require prior, free, express, unequivocal, and informed consent from the holder of personal data (Article 13(5), Amended PDPL; Articles 7 and 12, PDP Regulation). The PDP Regulation clarifies this as follows:

- **Prior.** The holder of personal data must consent before personal data collection or processing (Article 12(2), PDP Regulation).
- **Free.** The holder of personal data must give consent without error, bad faith, violence, or fraud affecting their will (Article 12(1), PDP Regulation).
- **Express and unequivocal.** The holder of personal data may demonstrate express and unequivocal consent verbally, in writing, or through technological means that clearly manifests consent, such as by clicking on an acknowledgement of consent (Article 12(3), PDP Regulation).
- **Informed.** In plain language, holders of personal data must have certain information communicated to them prior to collection, including:
 - the identity and contact details of the holder of a personal data bank, which other jurisdictions commonly refer to as data controllers, or manager of a personal data bank, which other jurisdictions commonly refer to as data processors;
 - the purposes for the personal data processing;
 - the identity of personal data recipients, if any;
 - the existence of the relevant data bank that will store the data, whether electronic or otherwise;
 - whether providing responses is compulsory or optional, especially regarding sensitive personal data;
 - the consequences of providing or refusing to provide personal data;
 - any national or cross-border personal data transfers, when applicable;
 - the storage period; and
 - the possibility to exercise their rights, including the rights to access, rectify, suppress, or oppose the processing, among other rights that the data protection law grants (see Question 13), and the means to do so.

(Article 12(4), PDP Regulation; for more on notice requirements for personal data holders, see Question 12.)

Withdrawing Consent

The holder of personal data can revoke their consent at any time without justification. The revocation will only

impact data processing that occurs after the holder of personal data withdraws consent. The revocation does not have retroactive effects. (Article 13(7), Amended PDPL; Article 16, PDP Regulation.)

Explicit Consent

For sensitive personal data, the holder of personal data must give explicit written consent for collection. Handwritten or digital signatures satisfy the written requirement (Article 13(6), Amended PDPL; Article 14, PDP Regulation). Additionally, holders of a personal data bank may only process sensitive data for concrete purposes in compliance with their activities or explicit aims (Article 8, PDP Regulation). For more on special rules for sensitive data, see Question 11.

Consent by Minors

Holders of a personal data bank must obtain consent from parents or legal guardians of minors younger than 14 (Article 27, PDP Regulation). However, holders of the personal data between the ages of 14 and 18 years can give consent, as long as the information provided to them has been expressed in a language that they can understand, except in cases where the law requires the assistance of their parents or legal guardians (Article 28, PDP Regulation).

10. If consent is not given, on what other grounds (if any) can processing be justified?

The [Personal Data Protection Law](#) (Law No. 29733), which [Legislative Decree 1353](#) amended (together Amended PDPL) (both in Spanish), does not require consent from the holder of personal data, which other jurisdictions commonly refer to as data subjects:

- When public entities collect and transfer personal data to perform activities within the scope of their functions and authority.
- When a publicly available source includes or will include the data.
- When the personal data relates to financial solvency and credit standing under the law.
- When the use falls under [Law No. 27332, Framework Law of the Regulatory Entities of Private Investment in Public Services](#) (in Spanish), which promotes competition in regulated markets, or similar regulations, if the use of the information does not violate the user's privacy.
- If necessary:
 - to execute a contractual or pre-contractual obligation when the personal data holder is a party to the contract; or
 - for the development and compliance of a scientific or professional relationship with the personal data holder.
- When related to health data, if necessary:
 - under risk circumstances, for the prevention, diagnosis, and medical or surgical treatment of the holder of personal data, provided that health professionals with professional secrecy obligations do the processing or the processing happens in health facilities;
 - for public health reasons if the Minister of Health qualifies those reasons; or
 - to conduct epidemiological or similar studies if the personal data is anonymized or de-identified (for more on anonymization and dissociation, see Question 3).
- When a political, religious, or union non-profit organization uses personal data that they collect from members if:
 - it relates to the organization's activities; and
 - the organization does not transfer the data without the members' consent.
- When the personal data is anonymized or de-identified.
- When the personal data is necessary to safeguard the holder of the personal data's legitimate interests.
- When the processing relates to:
 - anti-money laundering or terrorism financing prevention; or
 - other legal mandates.
- To exchange financial information among companies of the same business group:
 - to prevent money laundering or terrorism financing; or
 - for regulatory compliance reasons with adequate safeguards.
- When the processing is within a constitutionally valid exercise of the freedom of information.
- When another law or regulation provides an exemption.

(Article 14, Amended PDPL.)

Special Rules

11. Do special rules apply for certain types of personal data, such as sensitive data?

Under the [Personal Data Protection Law](#) (Law No. 29733), which [Legislative Decree 1353](#) amended (together Amended

PDPL), and [Personal Data Protection Regulation](#) (PDP Regulation) (all in Spanish), sensitive data is:

- Personal data regarding an individual's:
 - racial and ethnic origin;
 - personal income;
 - opinions regarding politics, religion, philosophy, or morality;
 - union membership;
 - physical or mental health;
 - sexual life;
 - physical, moral, or emotional characteristics;
 - facts or circumstances of emotional or family life; or
 - personal habits that correspond to the most intimate sphere.
- Biometric data that by itself can identify the owner.
- Analogous information that affects a person's privacy.

(Article 2(5), Amended PDPL; Article 2(6), PDP Regulation.)

For sensitive data:

- The holder of personal data, which other jurisdictions commonly refer to as a data subject, must give explicit written consent for processing. Handwritten or digital signatures satisfy the requirement. (Article 13, Amended PDPL; Article 14, PDP Regulation.)
- The processing's purpose must relate to activities of the holder of a personal data bank, which other jurisdictions commonly refer to as a data controller (Article 8, PDP Regulation).

For more on processing non-sensitive personal data, see Question 9 and Question 10.

Rights of Individuals

12. What information rights do data subjects have?

The [Personal Data Protection Law](#) (Law No. 29733), which [Legislative Decree 1353](#) amended (together Amended PDPL), and [Personal Data Protection Regulation](#) (PDP Regulation) (all in Spanish) require that all privacy notices expressly and clearly inform individuals of the certain information before collecting their personal data, including:

- The identity and contact details of the holder of a personal data bank or manager of a personal data bank. Other jurisdictions commonly refer to personal data bank holders as data controllers and personal data bank managers as data processors.

- The purposes for processing the individual's personal data.
- The parties who may or will receive the data.
- The existence of the relevant data bank, whether electronic or otherwise.
- Whether providing the personal data is compulsory or optional.
- The consequences of providing or refusing to provide personal data.
- The possibility of the holders of personal data to their rights, including the rights to access, rectify, suppress, or oppose the processing, among other rights that the data protection law grants. Other jurisdictions commonly refer to holders of personal data as data subjects. For more on other specific rights of holders of personal data, see Question 13.
- The retention period for the personal data.
- Any cross-border transfers of the personal data (see Question 20).

(Article 18, Amended PDPL; Article 12(4), PDP Regulation.)

The notice may be written or electronic. If electronic, a holder of a personal data bank may satisfy this obligation through its privacy policy. (Article 18, Amended PDPL.)

The PDP Regulation clarifies that publication of privacy policies is a form of compliance with the duty of information. It does not exempt holders of personal data banks or managers of personal data banks from any consent requirements. (Article 13, PDP Regulation; for more on consent, see Question 9).

Further criteria from the NAPDP may be found on the [Practical guide for compliance with the duty to inform](#) approved by Managerial Resolution N° 80-2019-JUS/DGTAIPD.

13. Other than information rights, what other specific rights are granted to data subjects?

In addition to notification rights (see Question 12), the [Personal Data Protection Law](#) (Law No. 29733), which [Legislative Decree 1353](#) amended (together Amended PDPL), and [Personal Data Protection Regulation](#), (PDP Regulation) (all in Spanish) give holders of personal data, which other jurisdictions refer to as data subjects:

- **The right to request information and access personal data.** The holder of personal data has the right to request certain information. The holder of personal data may request information on:

- the processing;
- the collection;
- the purposes or reasons for collection;
- who ordered the processing; and
- any cross-border transfers.

(Articles 18 and 19, Amended PDPL; Articles 60 and 61, PDP Regulation; see Question 12.)

- **The right to prevent disclosure of personal data.** The holder of personal data has the right to prevent the disclosure of personal data to third parties especially when it impacts the individual's fundamental rights. This right does not apply to disclosure to third-party data processors, which Peru's laws refer to as managers of personal data banks. (Article 21, Amended PDPL; for more on working with third parties, see Question 17.)
- **The right to object to personal data processing.** The holder of personal data may object to personal data processing for legitimate reasons relating to the individual. The holder of a personal data bank, which other jurisdictions commonly refer to as a data controller, and a manager of a personal data bank must then delete the personal data (Article 22, Amended PDPL; Article 71, PDP Regulation).
- **The right not to be subject to automated decision-making.** Holders of personal data have the right not to be subject to a decision based on automated processing with legal or significant effects based on personal data processing intended to evaluate certain aspects of their personality traits or behavior unless it occurs:
 - during the negotiation of a contract; or
 - in the process of hiring or incorporating someone into a public office.

(Article 23, Amended PDPL; Article 72, PDP Regulation.)

- **The right to update, include, rectify, or delete personal data.** The holder of personal data has the right to update, include, rectify, or delete personal data when:
 - the data is partially or totally inaccurate, incomplete, false;
 - there is an omission or error;
 - the data is no longer necessary or relevant for its collection purpose; or
 - the expiration date established for the data processing occurs.

(Article 20, Amended PDPL; Articles 64 to 67, PDP Regulation.)

If the holder of a personal data bank has transferred the personal data to a manager of a personal data bank, the holder of a personal data bank must communicate the respective deletion so that the manager can delete the information too. Also, the holder of a personal data bank must block the data bank during the deletion process so third parties may not access the affected information. (Article 20, Amended PDPL, Article 68, PDP Regulation.)

- **The right to be indemnified.** The holder of personal data has the right to be indemnified or to claim compensation for any damages that a data protection law infringement causes (Article 25, Amended PDPL; for other sanctions and remedies, see Question 26).

Whenever anyone denies a holder of personal data their rights, the individual may either file:

- A claim before the NAPDP (see Box, Regulator Details).
- A petition for the writ of habeas data before the judiciary.

(Article 24, Amended PDPL.)

Public administrations acting as personal data bank holders and managers may be able to limit personal data holders' access, deletion, and opposition rights in certain circumstances, such as:

- To protect the rights and interests of third parties.
- If it would hinder:
 - ongoing judicial or administrative actions related to tax or social security obligations or criminal investigations; or
 - health or environmental control functions.
- When other laws require it.

(Article 27, Amended PDPL.)

14. Do data subjects have a right to request the deletion of their data?

See Question 13.

Security Requirements

15. What security requirements are imposed in relation to personal data?

The [Personal Data Protection Law](#) (Law No. 29733), which [Legislative Decree 1353](#) amended (together Amended PDPL) (both in Spanish), requires holders of a personal data bank and managers of a personal data bank to adopt organizational, technical, and legal measures to

protect personal data against damage, loss, alteration, or unauthorized access or processing (Article 16, Amended PDPL). Other jurisdictions commonly refer to holders of a personal data bank as data controllers and managers of a personal data bank as data processors.

Holders of a personal data bank and managers of a personal data bank must also use security measures that correspond to the data it protects, such as sensitive data (Article 10, PDP Regulation; for more on sensitive personal data, see Question 11).

Holders of a personal data bank and managers of a personal data bank must store personal data in data banks that include protections, such as:

- Access controls and limitations.
- Identification and authentication procedures.
- Methods for conservation, backup, and personal data recovery.
- Authorization for personal data transfers and for reproduction or copies.
- Security measures for document storage and personal data transfers, including encryption, digital signatures, verification, or other measures aimed at providing protection and preventing manipulation of data.
- Measures to ensure that data cannot be recovered from destroyed copies or reproduction of documents.

(Articles 39 to 46, [Personal Data Protection Regulation](#) (PDP Regulation) (in Spanish).)

The PDP Regulation also requires personal data bank holders to ensure secure processing of children's personal data (Article 30, PDP Regulation). The only specific requirement in this regard, however, concerns consent (Articles 27 and 28, PDP Regulation; see Question 9).

The NAPDP issued a directive that establishes security measures for the management of personal data; however, these are not legally binding to holders of the personal data bank or managers of a personal data bank (see [National Authority for Personal Data Protection Directive on Security of Information No. 019-2013-JUS/DGPDP](#)) (in Spanish)).

For security measures related to third-party processing of personal data, see Question 17.

16. Is there a requirement to notify data subjects or the supervisory authority about personal data security breaches?

The [Personal Data Protection Law](#) (Law No. 29733), which [Legislative Decree 1353](#) amended (together Amended PDPL), and [Personal Data Protection Regulation](#) (PDP Regulation) (all in Spanish) do not

use the terms data controller or data processor. The Peruvian law refers to holders of personal data banks, which other jurisdictions commonly refer to as data controllers, and managers of personal data bank, which other jurisdictions commonly refer to as data processors.

The NAPDP issued a non-binding directive that recommends the holder of a personal data bank or manager of a personal data bank to inform holders of personal data, which other jurisdictions commonly refer to as data subjects, of any incident that significantly impacts their property or moral rights as soon as it confirms the incident (See [National Authority for Personal Data Protection Directive on Security of Information No. 019-2013-JUS/DGPDP](#) (Information Security Directive) (in Spanish)).

The Information Security Directive recommends holders of a personal data bank or managers of a personal data bank to provide individuals with the information, such as:

- A description of the incident.
- Details regarding the disclosed personal data.
- Recommendations to the holder of personal data.
- Any implemented corrective measures.

The Information Security Directive:

- Does not require or recommend notifying the NAPDP about a data breach.
- Recommends keeping track of all incidents, including setting minimum information requirements.

Processing by Third Parties

17. What additional requirements (if any) apply where a third party processes the data on behalf of the data controller?

The [Personal Data Protection Law](#) (Law No. 29733), which [Legislative Decree 1353](#) amended (together Amended PDPL), and [Personal Data Protection Regulation](#) (PDP Regulation) (all in Spanish) refer to holders of personal data banks, which other jurisdictions commonly refer to as data controllers. Any third party processing personal data on a holder of a personal data bank's behalf must:

- Process personal data according to the holder of a personal data bank's instructions and exclusively for the purpose set out in the agreement between the holder of a personal data bank and manager of a personal data bank. Other jurisdictions commonly refer to managers of personal data banks as data processors.
- Obtain the holder of a personal data bank's authorization to subcontract the processing of

personal data, except when the holder of a personal data bank and manager of a personal data bank previously agreed on the possibility of transferring data in their contract.

- Destroy the data once it fulfils all contractual obligations, unless the holder of a personal data bank gives an instruction to keep the data for a longer time where there is a possibility of future services related to the data. In any case, the data may be securely stored for no longer than two years.
- Implement organizational, technical, and legal measures to protect personal data against damage, loss, alteration, or unauthorized access or processing (see Question 15).
- Comply with the main obligations placed on holders of the personal data bank (see Question 8).
- Publicize any changes in their privacy policies or conditions of service dealing with consent if it means increasing processing powers.
- Allow the holder of a personal data bank to limit processing.

(Articles 16, 28, and 30, Amended PDPL; Articles 2(10) and 35 to 37, PDP Regulation.)

While the Amended PDPL and the PDP Regulation does not specify that an agreement between a holder of a personal data bank and a manager of a personal data bank needs to be in writing, it is highly recommended due to enforcement actions. Consent is also always necessary unless an exception applies (see Question 9 and Question 10).

Subcontracted third-party processors assume the same obligations as the manager of the personal data bank. In addition, subcontracted third-party processors will assume the same obligations as the holder of a personal data bank when either:

- The subcontracted third party uses the personal data for a purpose that the holder of a personal data bank has not authorized.
- The subcontracted third-party makes an unauthorized transfer of the personal data, even if it is for conservation purposes.

(Article 38, PDP Regulation.)

A holder of a personal data bank and a manager of a personal data bank have equal individual responsibility for violations (Article 38, PDP Regulation).

For more on personal data bank holders' main obligations, see Question 8. For more on cross-border data transfers, see Question 20.

Electronic Communications

18. Under what conditions can data controllers store cookies or equivalent devices on the data subject's terminal equipment?

Although the [Personal Data Protection Law](#) (Law No. 29733), which [Legislative Decree 1353](#) amended (together Amended PDPL) (both in Spanish), does not directly regulate cookies or location technologies, data protection laws and regulations apply if the cookies or location technologies collect or process personal data, including requirements on notice and consent. In those cases, the Amended PDPL's exceptions for obtaining consent from the holder of personal data also apply (Article 14, Amended PDPL). Other jurisdictions commonly refer to holders of personal data as data subjects.

For more on:

- The definition of personal data, see Question 3.
- Consent, see Question 9.
- Legal grounds to process personal data without consent, see Question 10.
- Information requirements for holders of personal data, see Question 12.

19. What rules regulate sending commercial or direct marketing communications?

There are no specific regulations covering commercial or direct marketing communications in the [Personal Data Protection Law](#) (Law No. 29733), which [Legislative Decree 1353](#) amended (together Amended PDPL), or [Personal Data Protection Regulation](#) (all in Spanish). However, it is important to consider that commercial or direct marketing communications, as any other data processing purpose, require specific consent to be legally executed.

Under the [Anti-Spam Law No. 28493](#) (in Spanish) (Anti-Spam Law), which regulates unsolicited electronic commercial communications, every unsolicited email originated in Peruvian territory must provide an opt-out mechanism to restrict further unsolicited emails (Articles 1, 5, and 6, Anti-Spam Law). Further details about the requirements under the Anti-Spam are outside the scope of this Q&A.

International Transfer of Data

Transfer of Data Outside the Jurisdiction

20. What rules regulate the transfer of data outside your jurisdiction?

The [Personal Data Protection Law](#) (Law No. 29733), which [Legislative Decree 1353](#) amended (together Amended PDPL) (both in Spanish), allow personal data transfers to other countries that provide an adequate level of protection, which means that the country provides at least the same level of data protection as Peruvian law provides. For countries that do not provide an adequate level of protection, cross-border personal data transfers may occur if the sender guarantees that the data processing will comply with the Amended PDPL. (Articles 11 and 15, Amended PDPL.)

However, an entity may transfer personal data to countries without an adequate level of protection or other guarantees in the certain situations, such as:

- The transfer occurs because of an international treaty to which Peru is party.
- International legal cooperation.
- International cooperation among intelligence agencies in the fight against terrorism, illicit drug trafficking, money laundering, corruption, human trafficking, among other organized crime.
- To execute a contractual relationship to which the holder of personal data is a party. Other jurisdictions commonly refer to the holder of personal data as a data subject. This may include activities such as user authentication, service improvement, technical support, maintenance, and billing, among others.
- Money or stock transfers made according to applicable Peruvian law.
- If medical prevention or diagnosis requires the transfer, or to provide healthcare or medical treatment. to manage healthcare services, or to conduct epidemiological studies, if the data undergoes adequate de-identification procedures (for more on anonymization and dissociation, see Question 3).
- The holder of personal data has given prior, free, express, unequivocal, and informed consent to the data transfer (for more on consent, see Question 9).
- The personal data transfer fulfills a scientific or professional relationship with the holder of personal data, if, the data is necessary for the development and compliance with the relationship.

- Other exceptions under the Amended PDPL that may be deduced from the law's guiding principles.

(Articles 12 and 15, Amended PDPL.)

Entities that transfer the data cross-border have the burden of demonstrating their compliance with the Amended PDPL and the [Personal Data Protection Regulation](#) (PDP Regulation) (in Spanish) (Articles 18 and 19, PDP Regulation).

All international data transfers require the recipient or importer of personal data to assume the same obligations as the exporter of personal data (Article 24, PDP Regulation). Exporters may use contractual clauses or other legal instruments establishing legal obligations, as well as the conditions in which the holder of personal data must consent to the processing of their personal data (Article 25, PDP Regulation).

The data exporter must notify the NAPDP about the cross-border transfer. This obligation can be fulfilled by declaring it in the data bank registration form. The NAPDP does not need to authorize to the personal data transfer. Companies may also transfer data cross-border to other companies within their economic group through a code of conduct that establishes the internal rules to protect the personal data, similar to what other jurisdictions call binding corporate rules (Article 31, Amended PDPL; Article 21, PDP Regulation). Companies must register any codes of conduct with the NAPDP. A [form](#) (in Spanish) is available on the NAPDP's website.

In addition, a holder of a personal data bank may request the opinion from the NAPDP about whether the cross-border data transfer complies with the Amended PDPL and PDP Regulation (Article 26, PDP Regulation). The NAPDP has a [form](#) (in Spanish) on its website.

21. Is there a requirement to store any type of personal data inside the jurisdiction?

The [Personal Data Protection Law](#) (Law No. 29733), which [Legislative Decree 1353](#) amended (together Amended PDPL) and the [Personal Data Protection Regulation](#) (all in Spanish) do not contain specific requirements on storing personal data in Peru. Sectoral laws may have data localization requirements, but they are outside the scope of this Q&A.

Data Transfer Agreements

22. Are data transfer agreements contemplated or in use? Has the supervisory authority approved any standard forms or precedents for cross-border transfers?

The [Personal Data Protection Law](#) (Law No. 29733), which [Legislative Decree 1353](#) amended (together Amended PDPL) (both in Spanish), allows for data transfer agreements and these agreements are in use. The [Personal Data Protection Regulation](#) (PDP Regulation) (in Spanish) states that data exporters may use contractual clauses or other legal instruments to establish, at least, the same legal obligations and other conditions (Article 25, PDP Regulation). For more on cross-border data transfers, see Question 20.

The NAPDP approved model contractual clauses as well as a guide for using them for international transfers (see [Directorial Resolution N. 0074-2022-JUS/DGTAIPD](#)).

23. For cross-border transfers, is a data transfer agreement sufficient, by itself, to legitimize transfer?

See Question 20, Question 22, and Question 24.

24. Must the relevant supervisory authority approve the data transfer agreement for cross-border transfers?

The [Personal Data Protection Law](#) (Law No. 29733), which [Legislative Decree 1353](#) amended (together Amended PDPL), and [Personal Data Protection Regulation](#) (all in Spanish) do not have any requirements to obtain prior approval of a data transfer agreement from the NAPDP (see Question 22). Although the law does not require the NAPDP's authorization, data exporters must fill out a form and submit it to the NAPDP to provide formal notice.

For more on:

- Data exporters, see Question 2.
- Notification to the NAPDP, see Question 7.
- Cross-border transfers, see Question 20.

Enforcement and Sanctions

25. What are the enforcement powers of the supervisory authority?

Under the [Personal Data Protection Law](#) (Law No. 29733), which [Legislative Decree 1353](#) amended (both in Spanish), the NAPDP has the power to:

- Represent the country before international data protection bodies.
- Cooperate with foreign data protection authorities.
- Manage the National Data Protection Registry.
- Publicize updated lists of public and private database personnel.

- Promote:
 - advertising and promotion campaigns on personal data protection; and
 - a culture of children's personal data protection.
- Supervise compliance with the data protection laws, including cross-border data transfers.
- Answer data protection queries.
- Issue:
 - authorizations, when appropriate;
 - technical opinions or binding standards for data protection; and
 - directives or best practices.
- Resolve data subject complaints and dictate precautionary or corrective measures.
- Obtain information to ensure compliance with the data protection laws and regulations.
- Impose:
 - fines for violations; or
 - corrective or precautionary measures to eliminate, avoid, or stop non-compliance.

(Article 33(20), Amended PDPL.)

For more on sanctions and remedies, see Question 26.

26. What are the sanctions and remedies for non-compliance with data protection laws?

The NAPDP may impose fines between 0.5 and 100 Tax Units. The applicable tax unit for 2020 is PEN4300, approximately USD1,213. (Article 39, [Personal Data Protection Law](#) (Law No. 29733), which [Legislative Decree 1353](#) amended (together Amended PDPL); Article 131, [Personal Data Protection Regulation](#) (PDP Regulation); Article 132, [Personal Data Protection Legislative Decree Regulation](#) ([Supreme Decree No. 019-2017-JUS](#)) (PDP Legislative Decree Regulation), (all in Spanish)). The PDP Legislative Decree Regulation details sanctions under the Amended PDP Law and PDP Regulation.

The amount of the fines varies depending on the type of infringement, including:

- A minimum fine of 0.5 to 5 Tax Units for a minor violation, such as processing personal data without adopting technical, organizational, and legal measures necessary to guarantee the information's security (see Question 14).
- A fine ranging from 5 to 50 Tax Units for serious violations, such as processing personal data without the holder of personal data's prior, free, express,

Data Protection in Peru: Overview

unequivocal, and informed consent unless otherwise provided by law (see Question 8). Other jurisdictions commonly refer to holders of personal data as data subjects.

- A fine ranging from 50 Tax Units to 100 Tax Units for very serious violations, such as collecting personal data through fraudulent, disloyal, or illicit means.

(Articles 38 and 39, Amended PDPL; Article 132, PDP Legislative Decree Regulation.)

The NAPDP determines the fine by applying the procedure described in the “Methodology for the Calculation of Fines regarding the Protection of Personal Data” approved by [Ministerial Resolution N° 0326-2020-JUS](#).

The amount of the total amount of the fine cannot exceed ten percent of the alleged offender’s gross revenue or earnings for the preceding year (Article 39, Amended PDPL).

In addition, the NAPDP may impose coercive fines, which must not exceed 10 Tax Units, to ensure compliance with accessory obligations of the main sanction. Civil and criminal liability, such as damages or breach of professional secrecy, may also arise as a result of data protection law violations (Article 40, Amended PDPL).

Regulator Details

National Authority for Personal Data Protection

W <https://www.minjus.gob.pe/registro-proteccion-datos-personales/>

Main areas of responsibility. The main regulatory agency in Peru is the National Authority for Personal Data Protection (NAPDP). The NAPDP is an agency within the Ministry of Justice and it has administrative, guiding, regulatory, supervisory, and sanctioning functions. The NAPDP has the following responsibilities:

- Represent the country before international instances in matters of personal data protection.
- Cooperate with foreign authorities in matters of personal data protection.

- Administer and keep updated the national data protection registry.
- Solve personal data protection complaints.
- Sanction personal data protection violations.

Online Resources

W <https://www.minjus.gob.pe/registro-proteccion-datos-personales/>

Description. This is the official website of the National Authority for Personal Data Protection. It provides relevant information, legislation, decisions, and other documents.

Contributor Profiles

Oscar Montezuma Panez, Director

Niubox

T +(511) 711-0001

E omontezuma@niubox.legal

W <https://niubox.legal/>

Professional qualifications. Lawyer, Peru, 2005

Areas of practice. Data protection; information and communication technology; intellectual property; telecommunications.

Fiorella Colonna, Privacy, Technology and Competition Leader

Niubox

T +(511) 711-0001

E fcollonna@niubox.legal

W <https://niubox.legal/>

Professional qualifications. Lawyer, Peru, 2011

Areas of practice. Data protection; cybersecurity, information and communications technology, unfair competition and advertising, consumer protection, free competition, intellectual property, personal data protection, digital business and technology contracts.

Legal solutions from Thomson Reuters

Thomson Reuters is the world’s leading source of news and information for professional markets. Our customers rely on us to deliver the intelligence, technology and expertise they need to find trusted answers. The business has operated in more than 100 countries for more than 100 years. For more information, visit www.thomsonreuters.com