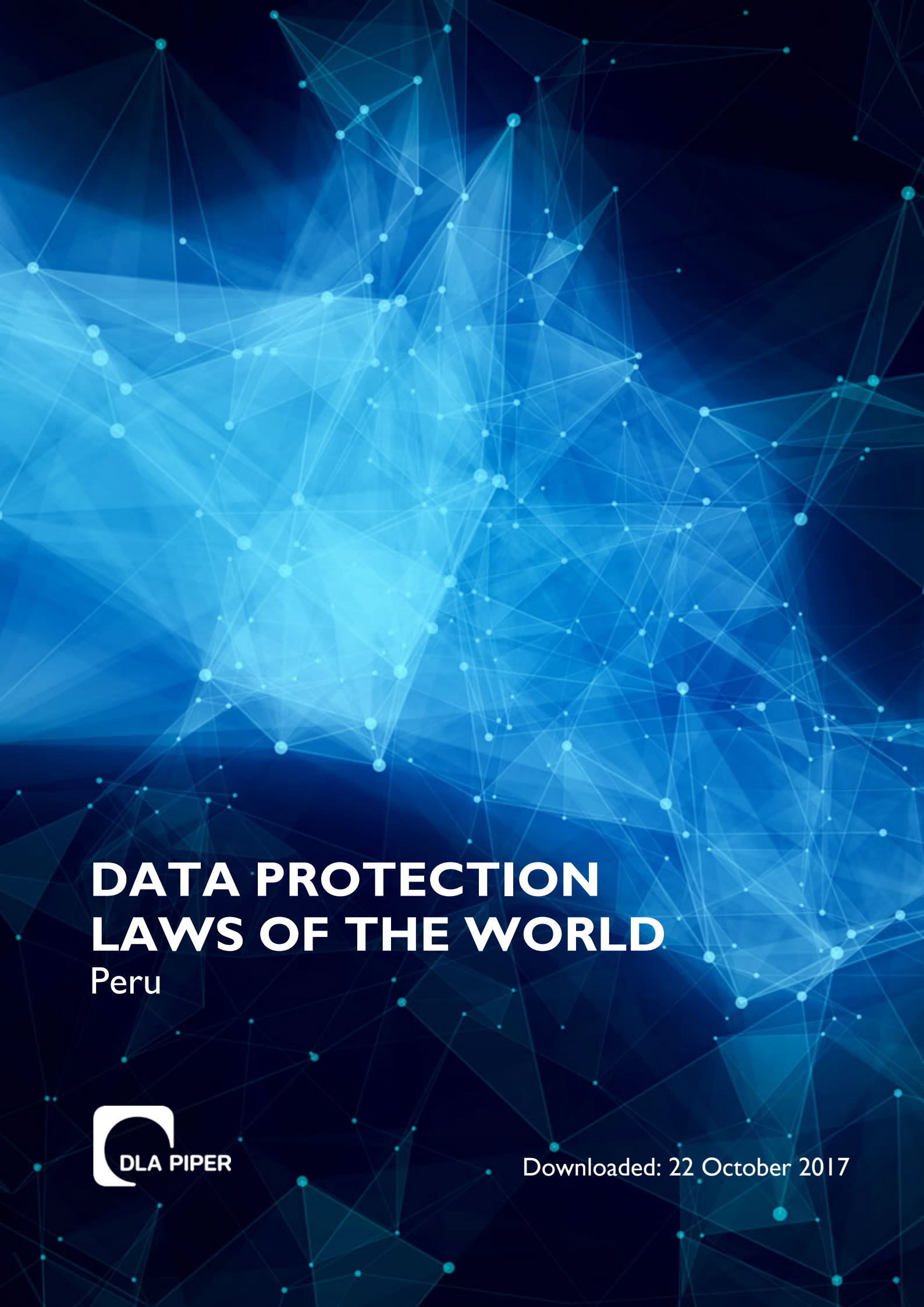
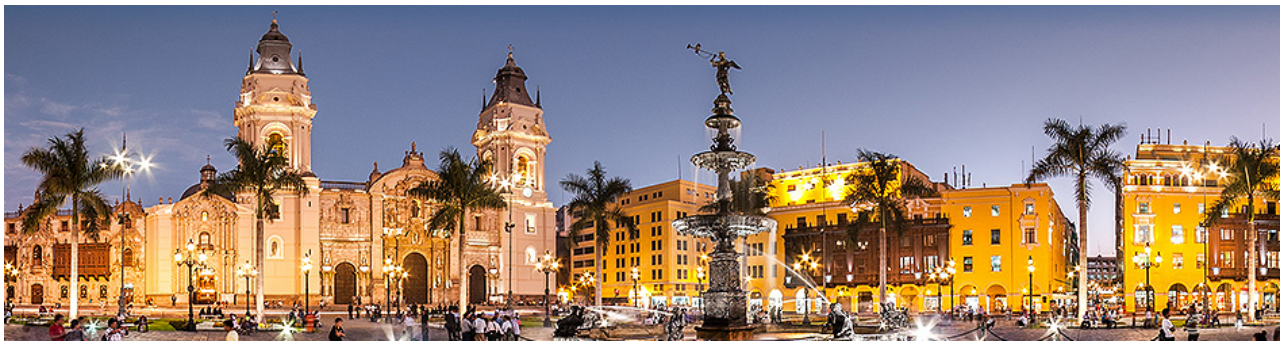


DATA PROTECTION LAWS OF THE WORLD

Peru

DLA PIPER

PERU



Last modified 24 January 2017

LAW

Personal data protection is governed in Peru by:

- the Personal Data Protection Law No. 29733 ('PDPL') published on July 3, 2011
- its regulations enacted by Supreme Decree 003-2013-JUS and published on March 22, 2013 (the 'Regulations'), and
- the Security Policy on Information Managed by Databanks of Personal Data enacted by Directorial Resolution N° 019-2013-JUS/DGPDP on October 11, 2013.

Although several provisions of the PDPL have been in force since July 4, 2011, most of the provisions of the PDPL only came into force on May 8, 2013 (30 business days after the issuance of the Regulations).

DEFINITIONS

Definition of personal data

The term "personal data" is defined broadly under the PDPL and its Regulations as all numerical, alphabetical, graphic, photographic, sound, or any other type of information concerning an individual which identifies or could be used to identify the individual through reasonable means.

Definition of sensitive personal data

"Sensitive data" is defined under the PDPL and its Regulations as biometric data which can identity someone; racial and ethnic background; income; political or religious opinions or creed; union membership; data related to health or sexual orientation and, in general, physical, mental and emotional characteristics, facts or circumstances of emotional or family life, and personal habits corresponding to the most intimate sphere of private life.

NATIONAL DATA PROTECTION AUTHORITY

The General Agency on Data Protection (Agency), part of the Ministry of Justice and Human Rights, is the National Authority for the Protection of Personal Data. The Agency oversees the PDPL.

Scipión Llona N° 350, Miraflores
Lima, Peru
T +511 204 8020 (annex 1030)
www.minjus.gob.pe/proteccion de datos personales

REGISTRATION

Public and private databases containing personal data must be registered with the National Registry for Personal Data Protection.

The following items shall also be registered in the Registry:

- codes of conduct, if any, that set standards for the processing of personal data, which are designed to ensure and improve the operation of information systems (the preparation of these codes by the owner or user of a database is voluntary)
- penalties, injunctive relief or remedies imposed by the Agency, and
- communications to the agency regarding cross-border transfers.

DATA PROTECTION OFFICERS

There is no requirement to appoint a data protection officer.

COLLECTION & PROCESSING

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

'Sensitive data' requires, additionally, that the data subject's consent be expressed in writing.

The consent of the data subject is not necessary when:

- the data are compiled or transferred for the fulfilment 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 No. 27489)
- a law is enacted to promote competition in regulated markets, under the powers afforded by the Framework Law for Regulatory Bodies of Private Investment on Public Services (Law No. 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 non-profit organization with a political, religious, or trade 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 or the data handler, or
- the data are used for other purposes recognized as exempt in law or in the Regulations.

TRANSFER

The transfer of personal data is subject to substantially the same restrictions as those applicable to collection and processing. Under the Regulations, a data transfer requires the consent of the data subject. The recipient of the data must assume the same obligations as the owner of the personal data.

However, in the case of cross-border transfers, the data holder generally must abstain from making transfers of personal data if the destination country does not afford 'adequate protection levels', which are equivalent to those afforded by the PDPL or in international standards.

If the destination country fails to offer 'adequate protection levels', the sender of the cross-border transfer of personal data must guarantee that the treatment of personal data meets 'adequate protection levels'. Generally, 'adequate measures' can be ensured via a written agreement that requires that the data will be protected in accordance with the requirements of the PDPL.

This guarantee is not necessary in the following cases:

- in accordance with international treaties in which Peru is a party
- international Judicial cooperation
- 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
- cross border transfers 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, or
- other exempt purposes established by the Regulations.

As with domestic transfers, the recipient must assume the same obligations as the owner of the personal data.

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 Directive regarding the security standards to which the processing of personal data must be subject. This Directive establishes different standards depending on the features of the database. The features that are relevant are the:

- number of data subjects whose data are contained in the database
- number of fields of the database (for example, name, address, phone number)
- existence of sensitive data, and
- owner of the database (an individual or entity).

BREACH NOTIFICATION

Under section 2.3.4.2 of the Security Policy on Information Managed by Databanks of Personal Data, enacted by Directorial Resolution N° 019-2013-JUS/DGPDP on October 11, 2013, the databank 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. Thus, certain data breaches trigger notice obligations. The minimum information to be provided in a notice includes:

- a description of the incident
- disclosed personal data
- recommendations to the data subject, and
- implemented corrective measures.

On the other hand, no breach notification to the General Agency on Data Protection is required.

ENFORCEMENT

The Agency is the government entity entrusted with enforcing the provisions of the PDPL. A breach of the obligations set forth therein gives rise to penalties.

The sanctions that could be imposed for breaching data protection standards vary depending on the nature or magnitude of the offense.

- The fine applicable to ordinary infringements ranges from approximately USD 686 to USD 6,859.
- The fine applicable to severe infringements ranges from approximately USD 6,859 to USD 68,592.
- The fine applicable to very severe infringements ranges from approximately USD 68,592 to USD 137,184.

It should be noted that notwithstanding the abovementioned amounts, in no scenario may a fine be greater than 10% of the alleged offender's gross revenues or earnings for the immediately preceding year.

The Agency is also authorized to resort to "coactive fines" which amount shall not exceed approximately USD 14,513. Coactive fines are those that are imposed in addition to the above mentioned fines if the offender, despite being found liable and sanctioned as a consequence thereof, fails to remedy the unlawful practice.

The above sanctions are applicable in addition to civil (e.g. damages) and criminal liability (eg breach of professional secrecy) that may arise pursuant to breaches of the PDPL.

ELECTRONIC MARKETING

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

Separately, the 'Anti Spam Law' No. 28493 and its regulations (Supreme Decree No. 031-2005-MTC) regulate specific aspects of electronic marketing.

These laws are applicable to any electronic mail message that originates in Peru and that qualifies as unsolicited commercial e-mail – defined broadly as e-mail that contains promotional commercial information regarding goods and services, including information regarding events, competitions and/or activities, traded, offered, sponsored or organized by company individuals.

Unsolicited commercial e-mails must contain:

- The word *PUBLICIDAD* (which means advertisement) at the beginning of the 'subject' field in the e-mail.
- Name or corporate name, complete domicile and e-mail address of the sender (including the complete name of a contact person).
- The inclusion of an e-mail address to which the receiver can send an e-mail in order to opt-out of receiving more unsolicited commercial e-mails, or another internet-based mechanism that enables opt-out.

A commercial e-mail is not considered unsolicited if it has been previously requested by the recipient (expressly and in writing) or if there is a prior contractual relationship with the recipient as long as the commercial communications sent refer to goods and services of the contracting company that are similar to goods or services contracted for.

Peru also offers a do not contact list. The Register of the Institute for Defence of Competition and Protection of the Intellectual Property (INDECOPI) called "Thanks ... do not insist", is intended for users that do not want to receive calls, text messages or e-mails. Users can register five phone numbers (land lines or mobile phones) and e-mail addresses at the INDECOPI webpage. Companies that use call centres, telephone calls systems, or send bulk text messages or e-mails, as well as those that provide telemarketing services must exclude from their lists all the numbers and addresses already registered at the INDECOPI webpage.

The 'do not contact list' registered before INDECOPI does not apply to communications that have been previously requested by

the recipient (expressly and in writing) or if there is a prior contractual relationship with the recipient, as long as the commercial communications sent refer to goods and services of the contracting company that are similar to goods or services contracted for.

The General Agency on Data Protection has recently interpreted that, in order to send a commercial e-mail to someone who is not protected by the "do not contact list", the sender must comply with the requirements of the Anti Spam Law or, alternatively, seek consent from the recipient.

ONLINE PRIVACY

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

KEY CONTACTS

Rodrigo, Elias & Medrano Abogados
www.estudiorodrigo.com

Jean Paul Chabaneix
Senior Partner
T +511 6191900
JPChabaneix@estudiorodrigo.com

Ximena Aramburu
Associate
T +511 6191900
Fbaldeon@estudiorodrigo.com

Francisco Baldeón
Associate
T +511 6191900
Fbaldeon@estudiorodrigo.com

DATA PRIVACY TOOL

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