Data protection in the Dominican Republic: overview

by Mary Fernández and Fernando J. Marranzini, Headrick Rizik Alvarez & Fernández, with Practical Law Data Privacy Advisor

Law stated as at 06 Aug 2019 • Dominican Republic

A Q&A guide to data protection in the Dominican Republic.

This Q&A guide gives a high-level overview of data protection rules and principles, including obligations on the data controller and the consent of data subjects, rights to access personal data or object to its collection, and security requirements. It also covers cookies and spam, data processing by third parties, and the international transfer of data. This Q&A also details the national regulator, its enforcement powers, and sanctions and remedies.

To compare answers across multiple jurisdictions, visit the Data protection Country Q&A tool.

Regulation

Legislation

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

General laws
The Constitution of the Dominican Republic 2015 (in Spanish) (Constitution):

- Sets out the basic tenets of the Dominican Republic's legal framework on privacy, recognizing individuals' right to intimacy and to live free from interference in their private lives as fundamental rights.
- Requires that **personal data** or information be treated according to certain principles, including the principles of:
  - reliability;
  - legality;
  - integrity;
  - security; and
  - purpose limitation.

(Article 44, Constitution.)

Law No. 172-13 for the Protection of Personal Data (in Spanish) (PDP Law) is the Dominican Republic's comprehensive data protection law. The PDP Law:

- Governs the collection, storage, safekeeping, use, and access rights of personal data recorded in files, databases, and registries for issuing public or private reports.
- Regulates the incorporation and operation of Dominican credit bureaus, defined as companies that collect, organize, store, conserve, provide, transfer, or transmit consumer data to provide credit scores or reports

and related goods and services. The PDP Law's provisions regulating credit bureaus are outside the scope of this Q&A.

Sectoral laws

Several sectoral laws address data protection and privacy in the Dominican Republic, including:

- Law No. 183-02 Monetary and Financial Law (in Spanish), which imposes on banks and other regulated financial institutions:
  - secrecy requirements;
  - a legal obligation to maintain confidentiality regarding deposits received from the public and refrain from revealing information in a detailed or segregated manner that could reveal the identity of their customers or account holders.
- The Dominican Monetary Board's Cyber Security and Information Security Regulations (in Spanish), which set out:
  - guidelines and obligations for financial entities and payment system participants to maintain information's integrity, availability, and confidentiality and the efficient functioning of technological infrastructure; and
  - prevention and management requirements for financial entities such as banks, savings and loan associations, and payment system participants.
- Law No. 53-07 on High Technology Crime (in Spanish), which protects:
  - the integrity of information systems and their components;
  - information or data stored in or transmitted through information systems;
  - transactions and commercial agreements executed through those means; and
  - the confidentiality of the above.
- Law No. 192-19 on the Protection of the Image, Honor and Integrity of Injured Persons and the Deceased (in Spanish), which expressly recognizes certain rights (including legal action) to protect individuals who have died or been injured in an accident from:
  - unlawful intrusions to their private lives;
  - the public disclosure of certain images; and
  - the appropriation of their name or likeness for commercial or similar purposes.
- Decree No. 230-18 approving the National Strategy on Cyber Security (in Spanish), which indicates that new cybersecurity-related regulations may be forthcoming.
- Law No. 42-01 on General Health (in Spanish), which provides that patients have the right to confidentiality of information related to their health files and admission to institutions providing public or private health services unless:
  - the patient authorises disclosure;
  - the collective interest requires the disclosure and the patient's dignity and rights are protected; or
  - a judicial order or special law requires disclosure.
- Law No. 200-04 on Free Access to Public Information (in Spanish), which provides that an organisation may deny an information request that affects an individual's preponderant private rights and interests, specifically if the request involves publication of personal data that invades an individual's privacy. In that case, the organization may provide personal data only if:
  - the individual expressly and unequivocally consents; or
  - a law requires publication.
- Law No. 136-03 Protection of Children's Rights Code (in Spanish), which specifies when someone may use a minor's personal data for physical identification, even against the minor's will.
- Law No. 11-92 Dominican Tax Code (in Spanish) which establishes that information provided by taxpayers, responsible parties, and third parties to the Tax Administration is reserved, and may only be used for the proper purposes of administration as authorised by law.
- Law No. 107-13 Administrative Procedure Law (in Spanish), which:
  - provides that Public Administration personnel who manage personal data must respect an individual's private life and integrity; and
  - prohibits the processing of personal data for unjustified purposes and its transmission to unauthorised persons.
- Law No. 137-11 Organic Law on the Constitutional Court and Constitutional Procedures (in Spanish), which

provides that every person is entitled:
  - to a judicial action to ascertain the existence of, and access to, data about that person stored in registries or banks of public or private data; and
  - to demand the suspension, rectification, updating, and confidentiality of false or discriminatory data.
- Law 55-93 on HIV/AIDS, which prohibits HIV/AIDS testing for work-related purposes other than anonymous epidemiological research studies that do not involve personal identification data.
- Decree No. 122-07 Regulation for the Registration of Criminal Record Data (in Spanish), which provides that bodies in charge of criminal files and records owe data subjects:
  - access to their own information;
  - accuracy and veracity of the data;
  - security and control of the files and records;
  - equality on the management of the information;
  - rectification and updating of information when appropriate; and
  - protection of the individuals' privacy.

Scope of legislation

2. To whom do the laws apply?

Law No. 172-13 for the Protection of Personal Data (PDP Law) applies to:

- Natural persons whose personal information is subject to data processing, known as **data subjects**. Legal persons, such as companies and limited liability partnerships, are excluded.
- Any person that engages in the treatment of personal data (see Question 4), referred to as **data controllers** (*Responsable del tratamiento*) and **data processors** (*Encargado del tratamiento*) where applicable under the PDP Law.

(Articles 4(4) and 6(1), (12), and (18), PDP Law.)

For more information on:

- Personal data , see Question 3 and Practice Note, Caribbean Data Protection Law: Overview: Data Controller, Data Processor, and Data Subject Defined.
- The treatment of personal data, see Question 4.
- Exemptions under the PDP Law, see Question 6.

3. What data is regulated?

Law No. 172-13 for the Protection of Personal Data (PDP Law) regulates personal data recorded in files, public records, data banks, or other technical means of **data processing**, whether private or public (Article 1, PDP Law).

Personal data is any numerical, alphabetical, graphic, photographic, acoustic, or other type of information concerning an identified or identifiable natural person (Article 6(9), PDP Law).

The PDP Law further classifies personal data into the following categories:

- **Specially protected data** (sensitive data) is personal data revealing:

  - racial or ethnic origin;
  - political opinion;
  - religious, philosophical, or moral convictions;
  - union affiliation; and
  - information relating to health or sexual life.
- **Health-related personal data** is personal data an individual's past, present, or future physical or mental health.
- Computer data is personal data submitted to electronic or automated treatment or processing.

(Article 6(8), (10), and (30), PDP Law.)

For information on processing personal data, see Question 4 and Practice Note, Caribbean Data Protection Law: Overview: Personal Data Defined. For more information on processing specially protected data, see Question 11.

4. What acts are regulated?

Law No. 172-13 for the Protection of Personal Data (PDP Law) applies to the treatment and subsequent public or private use of personal data.

Treatment is any operations and procedures, whether electronic, automated or otherwise, that allow for personal data processing, including:

- Collection, generation, preservation, extraction, or organisation.
- Storage or modification.
- Evaluation, blocking, or destruction.
- Transmission to third parties through communications, consultations, interconnections, or transfers.

(Article 6(21), PDP Law.)

For more information, see Practice Note, Caribbean Data Protection Law: Overview: Data Processing Defined.

5. What is the jurisdictional scope of the rules?

Law No. 172-13 for the Protection of Personal Data (PDP Law) applies to:

- The treatment of personal data inside the Dominican Republic.
- International transfers of personal data from the Dominican Republic.

(Articles 6(2) and 80, PDP Law.)

The Dominican Republic does not generally require an organization to appoint a designated individual, such as a data protection or privacy officer, to oversee the organization's compliance with legal obligations. However, there may be sector-specific obligations (see Question 8).

For more information, see Practice Note, Caribbean Data Protection Law: Overview: Jurisdictional Scope of Data Protection Laws and Requirements to Appoint Data Protection Officers.

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

Law No. 172-13 for the Protection of Personal Data (PDP Law) does not apply to:

- Personal data maintained by individuals exclusively for personal and domestic activities.
- Personal data maintained by security and intelligence agencies of the Dominican Republic in charge of preventing, processing, and prosecuting crimes.
- A deceased person's personal data.
- The treatment of legal entities' data (see Question 2).
- Legal entities' personnel files with the following limited employee information:
  - first and last names;
  - positions held;
  - physical and email addresses; and
  - work phone and fax numbers.

(Article 4, PDP Law.)

Notification

7. Is notification or registration required before processing data?

The Dominican Republic does not have a national data protection authority. Therefore, Law No. 172-13 for the Protection of Personal Data does not require notification or registration before processing personal data.

For more information on data subject consent requirements, see Question 9.

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 Law No. 172-13 for the Protection of Personal Data (PDP Law), data controllers must observe the following general principles:

- **Lawfulness.** Personal data may not be kept or used for purposes contrary to the law or public order.
- **Accuracy and quality of the information.** Personal data collected for treatment must be:
  - accurate, adequate, and relevant to the purposes for which it was collected;

  - properly updated if necessary;
  - suppressed, excluded, or substituted if it is inaccurate or incomplete; and
  - stored in a way that allows data subjects to exercise their legal rights to **access** the data.
- **Notification to data subjects.** If the treatment or transmission of personal data requires data subjects' consent, prior **notice** must be given indicating:
  - the purposes for which the data will be used;
  - any potential recipients of the data;
  - the existence of the database or files;
  - the data controller's identity and domicile; and
  - the data subject's right to exercise legal remedies to access, correct, or suppress the data.
- **Consent.** Data controllers must obtain data subjects' consent before the treatment or transfer of personal data unless an exception applies (see Question 9 and Question 10).
- **Data security.** Data controllers must adopt and implement **technical, organizational, and security measures** to guarantee the personal data's security and prevent alteration, loss, or potential unauthorized access.
- **Duty of professional secrecy.** Data controllers and all persons engaged in the treatment of personal data are subject to a duty of professional secrecy, which requires them to preserve and refrain from disclosing the data's confidentiality. This obligation survives the termination of the relationship between data controller and data subject.
- **Duty of loyalty.** Data controllers may not collect personal data through fraudulent, disloyal, or unlawful means.
- **The data's purpose.** Personal data may not be processed in a way that exceeds the determined, explicit, and legitimate scope and purpose for which it was obtained, often called **purpose limitation**.

(Article 5, PDP Law.)

The Dominican Republic does not generally require an organization to appoint a designated individual, such as a data protection or privacy officer, to oversee the organization's compliance with legal obligations. However, there may be sector-specific obligations (see Question 1). For example, financial institutions and payment systems administrators subject to the Dominican Monetary Board's Cyber Security and Information Security Regulations must appoint a Cyber Security and Information Safety Officer.

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

Under Law No. 172-13 for the Protection of Personal Data (PDP Law), data subjects must **consent** before their personal data is processed unless an exception applies (Article 4, PDP Law; see Question 10).

Consent is any free, unambiguous, specific, and informed manifestation through which data subjects agree to the processing of their personal data (Article 6(7), PDP Law). Consent therefore cannot be implied or inferred. Online consent that meets the PDP Law's statutory requirements may be appropriate in certain circumstances as determined on a case-by-case basis.

Under the Civil Code of the Dominican Republic (Civil Code), minors under 18 must be legally represented by their parents or legal guardians to give consent (Article 488, Civil Code).

For more information on notice requirements before consent may be obtained, see Question 8 and Practice Note, Caribbean Data Protection Law: Overview: Data Subject Consent Requirements.

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

Under Law No. 172-13 for the Protection of Personal Data (PDP Law), consent is not required for personal data treatment or processing if:

- The personal data is obtained:
  - from public sources;
  - in connection with the performance of state functions or under a legal obligation;
  - for lists for marketing purposes and limited to name, identification or passport number, tax identification, or other biographical information; or
  - from clients in relation to the activities of regulated financial intermediation entities and entities that develop tools for credit ratings for the evaluation of risk of the debtors of the commercial and financial system.
- The treatment or processing is:
  - derived from a professional, scientific, contractual, employment, or commercial relationship with the data subject; and
  - necessary to develop and fulfill that relationship.
- The treatment or processing is:
  - provided by law;
  - performed directly between state government agencies;
  - necessary for reasons of public health, emergency, or epidemiological studies, if the data subjects' identity is preserved through adequate dissociation mechanisms; or
  - done by public security and intelligence agencies responsible for preventing, persecuting, and punishing crimes if prior judicial authorization is obtained.
- The data controller applies an information dissociation process to ensure that the data subjects are not identifiable.

(Articles 5(4) and 27, PDP Law.)

Special rules

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

Law No. 172-13 for the Protection of Personal Data (PDP Law) provides special rules for specially protected or sensitive data (see Question 3).

A person generally cannot be compelled to provide specially protected or sensitive data involuntarily. Therefore, data controllers cannot create files, databases, or registries to store data that directly or indirectly reveals specially protected or sensitive data without the data subjects' free, conscious, and express consent.

Specially protected or sensitive data may be collected and processed without data subjects' consent however:

- By churches, religious associations, non-profit associations, hospitals, political organizations, and unions to keep records of their members or associates.
- If:
  - there is a legally recognized public interest in the collection or processing; or

- the data is collected or processed for statistical or scientific purposes when the data subjects cannot be identified.

Personal data related to:

- Racial origin, health, or sex life may be processed without a data subject's consent when necessary to provide prevent or treat an illness, provided that the data processing is carried out by a professional subject to professional secrecy rules.
- The commission of criminal offenses may only be included in personal data files and processed or communicated to public registries after a public judicial process has been filed.

(Articles 75 and 77, PDP Law.)

For more information, see Practice Note, Caribbean Data Protection Law: Overview: Sensitive Personal Data Processing.

Rights of individuals

12. What information should be provided to data subjects at the point of collection of the personal data?

Under Law No. 172-13 for the Protection of Personal Data (PDP Law), before processing personal data, data controllers must provide the following information to data subjects in a clear and express manner:

- The purposes for which the data will be processed.
- Any potential recipients of the data.
- The existence of the database or files.
- The data controller's identity and domicile.
- The data subject's right to exercise legal remedies to access, correct, or suppress the data.

(Article 5(3), PDP Law.)

The PDP Law does not specify how data controllers should send the required information to data subjects.

13. What other specific rights are granted to data subjects?

Under Law No. 172-13 for the Protection of Personal Data (PDP Law), data subjects are granted the following **rights**:

- **Right of consultation for data protection**. Data subjects have the right to take judicial action to determine whether their personal information is kept in a public or private database (Article 7, PDP Law).
- **Right of access**. Data subjects have the right:
  - to access their personal data stored in public or private databases; and
  - to know the purpose for which their data is used.

- (Article 10, PDP Law.)

- **Rights of rectification, correction, and exclusion**. Data subjects have the right to request that their personal data be **rectified**, amended, updated or excluded from databases or files. These rights are independent of one another and may be exercised individually. (Articles 8 and 9, PDP Law.)
- **Right to compensation**. Data subjects who suffer damages from a breach of the PDP Law are entitled to compensation (Article 16, PDP Law).
- **Habeas data action**. Data subjects have the right to request a habeas judicial action to ascertain the existence of personal data stored in files, records, or public or private databases derived from a commercial, labor, or contractual relationship with a public or private entity (Article 17, PDP Law).

For more information, see Practice Note, Caribbean Data Protection Law: Overview: Data Subject Rights.

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

Under Law No. 172-13 for the Protection of Personal Data (PDP Law), data subjects have the right to request that their personal data be excluded or **deleted** particularly when it is inaccurate or incomplete (Article 8, PDP Law).

On receipt of the data subject's request, data controllers have ten days to verify the data subject's deletion claim and delete the affected personal data. Data controllers may object to the request if:

- They are legally or contractually bound to store the affected data.
- Deleting the affected data would injure the rights or **legitimate interests** of third parties.

(Articles 15 and 24, PDP Law.)

Security requirements

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

Law No. 172-13 for the Protection of Personal Data (PDP Law) requires data controllers and processors treating or processing personal data to adopt and implement the necessary technical, organizational, and security measures to:

- Guarantee the data's security.
- Prevent alteration or loss of, or potential unauthorized access to, the data.

Controllers and processors treating or processing personal data must:

- Maintain the data under sufficiently secure conditions to prevent adulteration, loss, or unauthorized access.
- Adopt internal privacy guidelines and procedural manuals to ensure adequate compliance with the PDP Law.
- Limit access to the data to only authorized persons.

(Articles 5(5) and 13, PDP Law.)

The PDP Law also provides that data controllers, relevant professional associations, or trade groups formulate

templates for guidelines or codes setting out:

- Rules concerning the processes and equipment used to treat personal data.
- Other operational rules or standards.

There may be other sector-specific data security requirements (see Question 1). For example, while Law No. 53-07 on High Technology Crime does not require specific security measures or requirements, it does expressly provide that legal entities may be liable for damages when their negligence or their representatives' or employees' lack of vigilance results in the commission of any criminal felonies.

For more information, see Practice Note, Caribbean Data Protection Law: Overview: Security for Personal Data.

16. Is there a requirement to notify personal data security breaches to data subjects or the national regulator?

There is no general requirement under Law No. 172-13 for the Protection of Personal Data to notify data subjects or the Superintendency of Banks of a data security breach (see Box, Regulator details).

Processing by third parties

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

Law No. 172-13 for the Protection of Personal Data (PDP Law) does not impose additional requirements on **third parties** that process data on the data controller's behalf. However, the PDP Law's general data subject notice and consent requirements still apply (see Question 8 and Question 9).

The PDP Law does not expressly address whether data controllers are liable for the actions of third parties processing data on their behalf. However, any person engaged in the treatment of personal data (including collection, assignment, and processing) is subject to the PDP Law's requirements (Articles 5(3), 6(19), and 28, PDP Law).

For more information, see Practice Note, Caribbean Data Protection Law: Overview: Third Party Processing.

Electronic communications

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

Law No. 172-13 for the Protection of Personal Data (PDP Law) does not expressly prohibit or otherwise restrict the use of cookies or equivalent devices on the data subject's terminal equipment. However, the PDP Law's general data subject notice and consent requirements would apply (see Question 9 and Question 10).

For more information, see Practice Note, Caribbean Data Protection Law: Overview: Cookies.

19. What requirements are imposed on the sending of unsolicited electronic commercial communications (spam)?

Law No. 310-14 on Unsolicited Electronic Commercial Communications (SPAM) (in Spanish) (SPAM Law) regulates the sending of unsolicited electronic commercial communications (spam). A commercial communication is any data message sent to an indiscriminate number of people, without their due authorization, to directly or indirectly promote or market the image, goods, or services of a company, organization, or person undertaking a commercial, industrial, artistic, or professional activity (Article 3(2), SPAM Law). Under the SPAM Law, all commercial communications must include:

- The word publicity (*publicidad*) in the email's subject field.
- The sender's name, address, and telephone number or email address.
- An opt-out mechanism, such as an email address or link that allows the recipient to unsubscribe or indicate the desire to stop receiving the messages.

(Articles 4 to 6, SPAM Law.)

The SPAM Law generally prohibits direct or indirect sending of spam unless the recipient has given consent. Spam may be spent, however, when the recipient:

- Has a pre-existing commercial relationship with the sender; and
- Has not expressed a desire to unsubscribe or opt-out.

(Article 8, SPAM Law.)

If the recipient expresses a desire at any time to unsubscribe or opt-out, the sender must cease sending spam within two business days after the request (Article 5(4), Spam Law).

International transfer of data

Transfer of data outside the jurisdiction

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

Under Law No. 172-13 for the Protection of Personal Data (PDP Law), transfers of data outside the Dominican Republic may only be carried out when:

- The data subject freely authorizes the data transfer, or when the laws allow it.
- Exchanging medical data:
  - to treat a data subject; or
  - for an epidemiological investigation or reasons of health or public hygiene.
- Necessary for bank transfers or stock exchanges.
- The data transfer is:
  - agreed to or contemplated by international treaties, conventions, or free trade agreements signed by the Dominican Republic;
  - for purposes of international cooperation among intelligence agencies to combat organized crime, terrorism, human trafficking, drug trafficking, and other crimes;
  - necessary to perform a contract between the data subject and the data controller, or for the execution of pre-contractual measures;
  - legally required to safeguard the public interest, for the recognition, exercise, or defense of a right in judicial proceedings, or for tax or customs agencies to execute their purposes;
  - for providing or requesting international judicial assistance; or
  - is requested from a public database or registry by an international agency with a legitimate interest.

(Article 80, PDP Law.)

Companies that intend to transfer personal data to affiliates or subsidiaries outside of the Dominican Republic are subject to the same requirements.

For more information, see Practice Note, Caribbean Data Protection Law: Overview: Cross-Border Data Transfers.

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

Under Law No. 172-13 for the Protection of Personal Data (PDP Law), personal data collected in the Dominican Republic should be stored in the Dominican Republic (Articles 6(20) and 80, PDP Law).

International transfers of personal data stored in the Dominican Republic must meet statutory requirements (see Question 20).

Data transfer agreements

22. Are data transfer agreements contemplated or in use? Have any standard forms or precedents been approved by national authorities?

Law No. 172-13 for the Protection of Personal Data (PDP Law) does not contemplate the general use of data transfer agreements and no standard forms or precedents have been approved.

Under the PDP Law, however, users or subscribers of Credit Information Company (CIC) databases must sign a contract for the provision of services with the corresponding CIC (Article 52, PDP Law). These contracts are outside the scope of this Q&A.

23.Is a data transfer agreement sufficient to legitimise transfer, or must additional requirements (such as the need to obtain consent) be satisfied?

Law No. 172-13 for the Protection of Personal Data does not contemplate the use of data transfer agreements (see Question 22). Data subjects must consent to a data transfer unless an exception applies (see Question 9 and Question 10).

24. Does the relevant national regulator need to approve the data transfer agreement?

Law No. 172-13 for the Protection of Personal Data does not contemplate the use of data transfer agreements (see Question 22).

Enforcement and sanctions

25. What are the enforcement powers of the national regulator?

The Dominican Republic does not have a national data protection authority. However, the Superintendency of Banks of the Dominican Republic oversees and supervises credit bureaus under Law No. 172-13 for the Protection of Personal Data (see Regulator details).

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

Under Law No. 172-13 for the Protection of Personal Data (PDP Law), anyone suffering injury from a violation or breach of the PDP Law has the right to recover damages. The PDP Law specifically recognizes the following claims for damages:

- The unjustified refusal to allow a data subject to review, correct, or cancel their personal data stored in a database or registry.
- The refusal to amend or exclude data from a database or registry after the data subject has obtained a legal decision for amendment or exclusion.
- Seriously or repeatedly violating court-issued judgments.

(Article 85, PDP Law.)

In addition to any direct damages, law enforcement may assess a fine ranging from ten to fifty times the minimum wage for the following infractions:

- Wrongfully or intentionally inserting or causing the insertion of false information into a database.
- Wrongfully or intentionally providing false information contained in a database to a third party.
- Knowingly and unlawfully accessing a database or otherwise bypassing or breaching security (confidentiality) systems.
- Disclosing the personal data contained in a database to a third party, when such disclosing party was legally bound to maintain the confidentiality or secrecy of the data.

(Article 84, PDP Law.)

Any person violating the PDP Law may also be punished with correctional imprisonment of up to six months.

Finally, the PDP Law also provides for administrative sanctions and penalties that may be enforced by the Superintendency of Banks of the Dominican Republic against credit bureaus.

Law No. 53-07 on High Technology Crime (see Question 1) criminalizes:

- Unauthorized access or attempts to access an information system.
- Unlawful interception of or interference with transmissions of data or signals.
- The alteration or damaging of electronics system's data and components, a telematics system, or a telecommunications system for fraudulent purposes.

REGULATOR DETAILS

Superintendency of Banks of the Dominican Republic (*Superintendencia de Bancos de la República Dominicana*)
W www.sb.gob.do/

Main areas of responsibility.

- Supervises financial intermediaries to verify compliance with applicable legislation, requests the creation of provisions to cover risks, demands compliance with current legal and regulatory provisions, and imposes penalties for non-compliance.
- With respect to Law No. 172-13 for the Protection of Personal Data, empowered to take necessary actions to comply with the objectives and enforce the provisions of the law. Specifically, the Superintendency of Banks must assist and advise natural persons regarding the scope and the legal means available for the defence of their rights, inspect and supervise Credit Information Companies, and impose the corresponding administrative sanctions for legal violations.

ONLINE RESOURCES

W www.poderjudicial.gob.do/marco_juridico/leyes.aspx

Description. Official website of the Supreme Court of the Dominican Republic, which provides up-to-date text of all Dominican legislation. Only available in Spanish.

W www.consultoria.gov.do/consulta/

Description. Official website for the General Counsel for the Executive Branch, which provides up-to-date text of all the Dominican legislation. Only available in Spanish.

CONTRIBUTOR PROFILES

Mary Fernández, Partner

Headrick Rizik Alvarez & Fernández
T +1 809 473 4500

E mfernandez@headrick.com.do

W www.headrick.com.do

Professional qualifications. Admitted to the Dominican Bar Association (CARD); Bachelor of Laws (LL. B.), Universidad Nacional Pedro Henríquez Ureña, 1979; Master of Laws (LL.M) in Intellectual Property, John Marshall Law School of Chicago, 2016

Areas of practice. Agency and distribution; alternative dispute resolution; banking and finance; corporate and M&A; foreign investments; intellectual property; privacy and data security.

Non-professional qualifications. Postgraduate courses in Political Science and International Relations, Georgia State University, 1980

Recent transactions

- Advised international development banks in a US$60 MM financing for the construction of a 57 MW solar power plant.
- Advised international investment firm in the acquisition of a multinational gaming and leisure group.
- Advised investors in connection with the acquisition of a minority stake in the country´s largest wireless tower operator.
- Represented major pharmaceutical companies and industrial concerns as head of the firm's Intellectual Property department.

Languages. Spanish, English

Professional associations/memberships. Member, Dominican Bar Association (CARD); Board member, Chamber of Commerce of Santo Domingo (CCPSD); Arbiter and Board member of the Center for the Resolution of Controversies (CRC) of the Chamber of Commerce of Santo Domingo; Chair, Latin American Council of the International Section of the New York State Bar Association (NYSBA); National Ambassador, International Chamber of Commerce (ICC) for the Commission on Intellectual Property, representing the Dominican Republic; Former President and Chair of the Legal Committee, Board of Directors of the American Chamber of Commerce of the Dominican Republic (AMCHAMDR); Former President, Board of Directors of the Dominican Association of Intellectual Property, Inc. (ADOPI); Former President and current member of the Board of the Santo Domingo Technological Institute (INTEC); Member, International Trademark Association (INTA); Member and

Disciplinary Panel Judge, Inter-American Association of the Intellectual Property (ASIPI), and Arbiter and the President of its Mediation, Conciliation and Arbitration Committee

Fernando J. Marranzini, Senior Associate

Headrick Rizik Alvarez & Fernández
T +1 809 473 4500

E fmarranzini@headrick.com.do

W www.headrick.com.do

Professional qualifications. Bachelor of Laws (LL. B.), Universidad Iberoamericana (UNIBE), 2010; Master of Laws (LL.M) in Global Business Law, New York University, 2014; Master of Laws (LL.M) in Corporate & Financial Services Law, National University of Singapore, 2014; Dual Degree Master of Laws (LL.M) in Administrative Law from Universidad de Salamanca & Instituto Global de Altos Estudios en Ciencias Sociales, 2015

Areas of practice. Banking and finance; corporate and M&A; privacy and data security; project finance; regulatory matters and compliance.

Recent transactions

- Advised an international food delivery service company in the acquisition of a leading local delivery service company.
- Advised international investment firm in the acquisition of a multinational gaming and leisure group.
- Advised investors in connection with the acquisition of a minority stake in the country's largest wireless tower operator.
- Regularly advises international clients in connection with compliance with local laws, including financial, banking, insurance and data protection regulations.

Languages. Spanish, English

Professional associations/memberships. Member, Dominican Bar Association (CARD); Member, New York State Bar Association; Member, National Association of Young Entrepreneurs, Inc. (ANJE)

