Dominican Republic - Data Protection Overview

March 2024

1. Governing Texts

1.1. Key acts, regulations, directives, bills

The right to personal data protection finds its foundation in Article 44 of the Dominican Constitution (only available in Spanish here), specifically addressing the right to intimacy and personal honor.

In 2013, the Congress of the Dominican Republic enacted Law No. 172-13 on Protection of Data (only available in Spanish here) ('Law No. 172-13'), which protects and regulates personal data located in files, public registries, data banks or other public or private data storage methods. Notably, this legislation also outlines the operational framework for Credit Bureau Companies, specifically concerning financial purposes.

Furthermore, in the Dominican Republic, alongside Law 172-13, there are additional laws and regulations that, while not exclusively focused on the protection of personal data, incorporate relevant provisions for privacy and the handling of personal information. The following regulations further enhance the legal landscape in this area:

- Law No. 126-02 on Electronic Commerce, Documents and Digital Signs (only available in Spanish here) ('Law No. 126-02'): this law, governs electronic commerce and complements the provisions outlined in Law No. 172-13, ensuring a comprehensive approach to personal data protection;
- Law No. 358-05 on the Protection of the Rights of Consumers or Users (only available in Spanish here) ('Law No. 358-05'): overseeing consumer rights, this law plays a pivotal role. Administered through the National Institute of Consumer Protection ('Pro-Consumidor'), it manages the relationship between consumers and local businesses, with a specific emphasis on safeguarding personal data;
- Resolution No. 055-06 on Complementary Regulation to Law No.126-02 on the Protection of Personal Data by Regulated Entities (only available in Spanish here) ('Resolution No. 055-06'): issued by the National Institute of Telecommunications ('INDOTEL'), this resolution establishes the regulatory framework applicable to the processing of personal data of consumers and users by regulated entities. Regulated entities, as defined by this regulation, include certification entities, providers of electronic signature services, and registration units, as well as service providers or infrastructure providers

operationally linked to these entities to the extent of their contractual relationship;
- Law No. 14-94 Code for the Protection of the Rights of Boys, Girls, and Adolescents (only available in Spanish here) ('Law 14-94'): governing the processing of minors' personal data; and
- Law No. 53-07 on High-Tech Crimes and Offenses (only available in Spanish here) ('Law No. 53-07'): focusing on technology-related crimes and felonies, brought an additional layer of protection against personal data-related offenses.

1.2. Guidelines

Resolution No. 055-06 aims to establish a regulatory framework that ensures the protection of users' personal data within the telecommunications sector. This includes regulating how entities regulated by INDOTEL should handle users' personal information, ensuring its privacy and security. Resolution No. 055-06 is grounded in fundamental data protection principles, such as transparency in information usage, obtaining the data subject's consent for processing, ensuring the security of personal data to prevent unauthorized access, and holding regulated entities responsible in case of non-compliance. Entities regulated by INDOTEL, including telecommunications service providers, are mandated to adopt appropriate technical and organizational measures to protect personal data. This involves implementing clear privacy policies, appointing data protection officers, and reporting security incidents affecting personal data. Resolution No. 055-06 reinforces the rights of data subjects, encompassing the right to be informed about the use of their personal data, the right to access their data, the right to rectification and deletion, and the right to object to the processing of their data for specific purposes.

INDOTEL is responsible for overseeing compliance with Resolution No. 055-06, with the authority to impose sanctions for violations of personal data protection. This includes conducting inspections and evaluating the security measures implemented by regulated entities.

1.3. Case law

There is currently no case law regarding data protection. The existing precedent solely rely on general procedures for *habeas data* claims and lack any court interpretation that might alter or complement the existing legal provisions related to data protection.

2. Scope of Application

2.1. Personal scope

Law No. 172-13 applies to any natural or legal person, whether public or private, engaged in the processing of personal data, registered in any database subject to processing. Additionally, it extends to any subsequent use of this data in both public and private domains.

2.2. Territorial scope

Law No. 172-13, as stated in Article 3, declares itself a law of public order Law and is applicable across the entire national territory of the Dominican Republic.

2.3. Material scope

Law No. 172-13 on the Protection of Personal Data in the Dominican Republic has a broad material scope and focuses on the comprehensive protection of personal data. The fundamental aspects of the material scope of Law No. 172-13 include:

- personal data: Law No. 172-13 applies to any information concerning identified or identifiable individuals, encompassing data such as names, identification, contact information, financial details, and sensitive data (e.g., health-related information);
- processing methods: Law No. 172-13 covers personal data recorded in files, public records, databases, and other means, both in physical and digital formats;
- data controllers and processors: Law No. 172-13 establishes obligations for those handling personal data, ensuring that the processing is carried out in a fair, legal, and transparent manner;
- rights of data subjects: Law No. 172-13 guarantees fundamental rights to individuals regarding their personal data, including access, rectification, cancellation, and opposition to the processing of their data; and
- security measures: Law No. 172-13 mandates the implementation of appropriate technical and organizational measures to protect personal data against unauthorized access, alteration, loss, or improper processing.

3. Data Protection Authority | Regulatory Authority

3.1. Main regulator for data protection

In general, the Dominican Republic lacks a centralized regulatory body specifically dedicated to data protection. However, specific entities indirectly oversee data protection for individuals. Notably, these include:

- Pro-Consumidor;
- the Bank Superintendency; and
- INDOTEL.

3.2. Main powers, duties and responsibilities

The entities listed above shoulder indirect duties and responsibilities pertaining to data protection. The Pro-Consumidor oversees the interaction between local businesses and consumers, encompassing the safeguarding of their data. The Bank Superintendency regulates the relationship between Credit Bureau Companies and Data Subjects.
The INDOTEL oversees telecommunication companies and, in principle, governs data processing between these entities and their users.

4. Key Definitions

Data controller: refers to any public or private individual who stores personal data (Article 6 of Law No. 172-13).

Data processor: encompasses any public or private individual who processes and transfers personal data to and from the Dominican Republic (Article 6 of Law No. 172-13).

Personal data: refers to any numerical, alphabetical, graphic, photographic, acoustic, or any other type of data related to an identifiable individual (Article 6 of Law No. 172-13).

Sensitive data: any personal data that may reveal political opinions, religious and moral convictions, union affiliation, health and sexual information (Article 6 of Law No. 172-13).

Health data: encompasses any information regarding past, present and future physiological or mental health status (Article 6 of Law No. 172-13).

Biometric data: Law No. 172-13 does not define the concept of biometric data.

Pseudonymization: Law No. 172-13 does not define the concept of pseudonymization.

Data subject: refers to any identifiable individual whose information is subject to data processing within a database method (Article 6 of Law No. 172-13).

5. Legal Bases

5.1. Consent

According to Law No. 172-13, processors and controllers are required to obtain consent from the data subject to handle and process sensitive data (Article 76 of Law No. 172-13). The processing and transfer of personal data requires explicit, written consent from the data subject, with this consent being highlighted when provided along with other statements. State investigative and intelligence agencies are exempt from this consent requirement but must obtain prior authorization from a competent judicial authority.

Entities contracting services with Credit Information Societies ('CIS') must obtain explicit, written consent from data owners before requesting a credit report. Users are responsible for collecting and retaining permissions for six months from the signing date. Users must maintain absolute confidentiality regarding the content of credit reports, and any breach of confidentiality makes the user solely responsible for their actions.

5.2. Contract with the data subject

The data subject's consent will not be required when the data arises from a contractual, scientific, labor, or professional relationship with the data subject and is required for its development (Article 27 of Law No. 172-13). Furthermore, the data subject's consent is not required if the personal data is received in relation to the operations carried by a financial entity through a Credit Bureau Company to evaluate credit risks.

5.3. Legal obligations

Data processors and controllers are obligated to ensure the safety of stored data, implementing all necessary measures to guarantee the protection of the subject (Article 5 (5) of Law No. 172-13). Data processors and controllers also have the responsibility to rectify

or erase any inconsistent information within the stored data if required by the subject (Article 8 of Law No. 172-13).

Additionally, the data subject's consent is not needed if it is required by law or if it is collected through the exercise of functions inherent to the faculties of the local government or through a legal obligation.

5.4. Interests of the data subject

Law No. 172-13 does not foresee the interests of the data subject as a legal basis for processing but a data subject's consent is not required in the following instances:

- if the data is related to the subject's health and is required for public health emergencies, in which case, sensitive data must be safeguarded through the appropriate dissociation mechanisms; and
- if it is collected for marketing purposes (only if this data includes general information of the subject such as name, passport number, etc.);

5.5. Public interest

Law No. 172-13 establishes that certain data can be published, updated, and accessible through public registries (Article 6(14) of Law No. 172-13). This does not include sensitive data (Article 6(14), Article 45, and Article 75 of Law No. 172-13). Furthermore, the data subject's consent is not necessary if data is obtained from a public source or if it is processed directly through government agencies.

5.6. Legitimate interests of the data controller

Law No. 172-13 does not foresee the legitimate interests of the data controller as legal basis for processing.

5.7. Legal bases in other instances

Consent from the data subject is not required if a dissociation mechanism has been applied and the subject is no longer identifiable through the data.

6. Principles

Law No. 172-13 is grounded in the principles outlined below:

Legality of personal data files

Personal data files must comply with local law and public order, duly recorded and adhered to the principles established in Law No. 172-13.

Data quality

The processing of personal data must adhere to the following guidelines:

- personal data collected must be certain, adequate, and relevant to the scope and purpose for which was obtained;
- data must be accurate and updated if necessary;
- incomplete or inaccurate data must be deleted, replaced, or completed by the controller/processor; and
- data must be stored in a way that allows the exercise of the right of access by its owner.

Data security

Data controllers and processors must implement technical and organizational measures to protect data and prevent alteration, loss, unauthorized processing, consultation, or access. It is prohibited to record data in files that do not meet technical standards of integrity and security. Data providers, CIS, and users are urged to adopt technical measures to safeguard credit history data in CIS databases. It is also required that CIS take measures to protect their databases against natural risks such as accidental loss or destruction and human risks such as unauthorized access.

Confidentiality

This principle addresses the duty of secrecy in the processing of personal data, stating that those involved in the process must maintain professional secrecy and the obligation of confidentiality. These obligations persist even after ending relationships with the data subject or the data controller, unless lifted by a court order or for well-founded reasons related to public security, national defense, or public health. The duty of secrecy implies that individuals or entities recognized as users of CIS must maintain confidentiality regarding information related to the data subject's credit history, disclosing it only to competent authorities. Additionally, the disclosure and reproduction of reports of any kind from a CIS in mass media are prohibited.

Loyalty

All collection of personal data must adhere to appropriate legal means.

Data purpose

Personal data will only be collected for processing when it is deemed appropriate, relevant, and not excessive in relation to the intended purpose.

7. Controller and Processor Obligations

7.1. Data processing notification

Generally, there are no specific provisions regarding data processing notification requirements.

7.2. Data transfers

As per Article 80 of Law No. 172-13, the transfer of personal data of any kind to countries or international or supranational organizations, requiring the consent of the data subject, will only be carried out when:

- the data subject, freely and consciously, consents to the transfer of data;
- the transfer involves the exchange of medical data when required for the treatment of the affected subject, an epidemiological investigation, or for reasons of public health or hygiene;
- in the case of bank or stock transfers, it relates to respective transactions and is in accordance with applicable legislation;
- the transfer of data has been agreed or contemplated within the framework of international treaties or agreements, and in the free trade agreements of the which the Dominican Republic is a part of;
- the transfer of data is aimed at international cooperation between intelligence agencies for the fight against organized crime, terrorism, human trafficking, drug trafficking, and crimes;
- the data transfer is necessary for the execution of a contract between the owner of the data and the person responsible for the treatment, or for the execution of pre-contractual measures;
- the legally required data transfer is for the safeguarding of public interest or for the recognition, exercise, or defense of a right in a judicial process or requested by a tax or customs administration for the fulfilment of their powers;

- the data transfer is carried out to provide or request international judicial assistance; or
- the data transfer is carried out at the request of an international organization with a legitimate interest from a public registry.

7.3. Data processing records

As mentioned above, data controllers and processors must record all personal data in a way that is easily accessible to the data subject and must implement all the necessary measures to prevent illicit access to such data.

7.4. Data protection impact assessment

Law No. 172-13 does not establish requirements or recommendations for data controllers and processors to carry out data protection impact assessments. However, Resolution No. 055-06 states that information systems and facilities for processing personal data shall undergo, at least every two years, an internal or external audit to verify compliance with security measures.

7.5. Data protection officer appointment

Law No. 172-13 does not establish requirements for data controllers and processors to appoint a data protection officer. However, Resolution No. 055-06 states that regulated entities shall appoint one or more security officers responsible for coordinating and overseeing the measures defined in the Security Documents. For Resolution No. 055-06, 'Security Documents' refers to the mandatory documents that regulated entities are required to develop and implement. These documents outline security regulations applicable to personnel with access to personal data and the information systems responsible for processing them.

7.6. Data breach notification

Law No. 172-13 does not establish specific requirements for notifying a data breach. However, Resolution No. 055-06 stipulates that entities must have an incident notification and management procedure. According to Resolution No. 055-06 'incident' is defined as any anomaly that affects or could affect the security of data.

7.7. Data retention

The retention of personal data must be accurate and should be updated if deemed necessary by the data subject. According to Article 17 of Law No. 172-13, data subjects may seek a *habeas data* remedy before the Courts of the Dominican Republic to protect their personal information from data controllers or processors. If the Courts determine that the data subject's rights and information are being compromised, they may instruct the data controller to rectify or delete the subject's personal data.

7.8. Children's data

Article 79 of Law No. 172-13 stipulates that the processing of data for individuals under the legal age is subject to the provisions of Law No. 14-94, which specifically regulates the protection of children.

7.9. Special categories of personal data

Law No. 172-13 explicitly addresses special categories of personal data, specifically referring to health-related data, criminal offense data, and data concerning minors.

7.10. Controller and processor contracts

Law No. 172-13 does not establish specific requirements for a contract to be in place between a controller and a processor. However, Resolution No. 055-06 stipulates that the contract between a data controller and a processor should:

- be in writing and include the signatures of all parties, allowing the use of digital documents or data messages with digital signatures;
- clearly specify the characteristics of services to be performed by the data processor;
- state that the data processor will only process personal data according to the instructions of the data controller;
- acknowledge the data controller's responsibility before data subjects and regulatory authorities;
- regulate that the data processor will not disclose personal data for any reason other than fulfilling the data controller's instructions;
- restrict the data processor from carrying out any data processing not explicitly outlined in the contract;
- define security measures the data processor must implement to comply with regulations; and
- address subcontracting by requiring a separate contract with third-party subcontractors, subject to the same conditions as the main contract and approved by the data controller before signing.

8. Data Subject Rights

8.1. Right to be informed

The right to be informed is stipulated in Section 3, Article 5 of Law No. 172-13.

When personal data is collected and consent is required, the data controller or processor must inform the data subject of the following:

- the purpose for which the data will be used and possible recipients;
- the existence of the file, registry, data bank and the identity of the controller/processor; and
- the right of the subject to access, rectify, and delete personal data.

8.2. Right to access

The right to access is stipulated in Article 10 of Law No. 172-13.

8.3. Right to rectification

The right to rectification is stipulated in Article 14 of Law No. 172-13.

8.4. Right to erasure

The right to erasure is stipulated in Article 13(3) of Law No. 172-13.

8.5. Right to object/opt-out

The right to object/opt-out is stipulated in Articles 8 and 9 of Law No. 172-13.

8.6. Right to data portability

Not applicable.

8.7. Right not to be subject to automated decision-making

Not applicable.

8.8. Other rights

Other rights, such as the right to verify data and the right to be indemnified, are covered in Title I, Section I, starting in Article 7 of Law No. 172-13.

9. Penalties

In general, anyone who suffers damage due to non-compliance with the provisions in Law No. 173-12 has the right to be compensated in accordance with the Law. However, certain cases may result in civil or criminal offenses.

Civil offenses

- denying, without legal bases, a request submitted by a data subject to review, rectify, or cancel personal data;
- refusing to rectify or cancel the information of a data subject after the latter has obtained a favorable ruling by a Court of the Dominican Republic; or
- committing a serious or repeated violation of the enforceable rulings issued by the Courts of the Dominican Republic.

Criminal offenses:

- accessing personal data of the subject without obtaining consent, punishable by a fine of 10 to 50 current minimum wages;
- using or providing a credit report for the purpose of committing a crime, resulting in a penalty equivalent to correctional imprisonment of six months to two years;
- a user of a Credit Bureau company using the credit report for purposes other than those consented by the data subject, facing a fine ranging from 10 to 100 minimum wages;
- fraudulently accessing the database of a Credit Bureau company to obtain and use any type of report, leading to a fine between 20 to 100 current minimum wages;
- violating the provisions of Law 172-13, punishable by correctional imprisonment of six months to two years and a fine of 100 to 150 minimum wages. The same sanction applies to anyone who, outside the purposes established in the law, discloses, publishes, reproduces, transmits, or records the partial or total content of a report of any type from a Credit Bureau company, referring to a data subject, in any mass media, whether print, television, radio, or electronic.

9.1 Enforcement decisions

As Law No. 172-13 is of recent application, and after verifying public registries, there have not been any public enforcement decisions sanctioning individuals under the Law.

Urania Paulino

PALLERANO NADAL Law & Consulting

Urania Paulino has more than 20 years of experience, concentrating her professional practice in the areas of foreign investment, corporate and business law, banking and finance, consumer law, competition law, customs law, tourism, free trade agreements, distribution relations, franchises, free zones, international trade, mergers and acquisitions and energy and renewable energy.

She has assisted JetBlue Airways Corporation in the opening of new routes, as well as in all regulatory and safety matters to ensure the proper functioning of its operations in the country. She also represented Dominican Lawyers Guild during the negotiations of the Free Trade Agreement between Central America and the Dominican Republic, protecting the interests of Dominican lawyers. She helped prestigious international brands such as Louis Vuitton, Swarovski, L'Oreal, Volvo, Fiat, Daimler, General Electric, and Procter & Gamble, among others, in matters related to distribution and franchises. She also assisted several international companies in their establishment in the country, specifically a gas compression plant and a liquor aging company. She was part of the legal team that advised the Food and Beverage Industry Association of the Dominican Republic, Inc. in the process initiated before the Regulatory Commission for Unfair Commercial Practices regarding the implementation of safeguard measures on imports of glass containers and bottles of all origins. This is one of the first cases presented before this regulatory committee in accordance with the provisions of Law No. 1-02 on unfair commercial practices and safeguard measures.

upaulino@pellerano.com

Sebastian Linera Garcia

PELLERANO NADAL Law & Consulting

Sebastián has experience in sports law, corporate law, intellectual property law, corporate law and financing deals for mergers and acquisitions and foreign investment projects.

Sebastián is an associate attorney with experience in corporate and sports law. He has assisted companies such as Barrick Gold Corporation in the due diligence process prior to the joint venture with Precipitate Dominicana in order to acquire a piece of the Pueblo Grande Project. He also formed part of the team that

took part on the due diligence for the sale of Tabacalera de García, part of Industrial Brands. He has assisted Whitehaven Holdings in several financing deals obtained for their mining concessions.

Sebastián has also lead the legal team formed by the Normalization Committee of the Dominican Football Federation (FEDOFUTBOL), named by FIFA. Said team was directly responsible in the legal incorporation and adequation under law 122-05 of more than 150 clubs and 20 football associations nationwide. He also worked with FIFA in order to modify the By-Laws of FEDOFUTBOL and its member associations, applying the best international governance practices. As Legal Director, he organized the elections for FEDOFUTBOL and its member associations. He currently serves as a member of the Electoral Committee of FEDOFUTBOL. He also serves as Executive Vicepresident of the International Law Students Association (ILSA), chapter PUCMM.

slinera@pellerano.com