ISSN 1682-7511

OFFICIAL GAZETTE

OF THE REPUBLIC OF CUBA

MINISTRY OF JUSTICE

Information in this issue

Official Gazette No. 90 Ordinary of August 25, 2022

NATIONAL ASSEMBLY OF PEOPLE'S POWER

Law 149/2022 "On Personal Data Protection".

(GOC-2022-832-O90) MINISTRY

Ministry of Communications

Resolution 58/2022 "Regulations for the Security and Protection of Personal Data in Electronic Support" (GOC-2022-833-O90)

ISSN 1682-7511

OFFICIAL GAZETTE

OF THE REPUBLIC OF CUBA

MINISTRY OF JUSTICE

REGULAR EDITION HAVANA, THURSDAY, AUGUST 25, 2022 YEAR CXX

Web Site: http://www.gacetaoficial.gob.cu/-Calle Zanja No. 352 corner Escobar, Centro Habana
Telephone numbers: 7878-4435 y 7870-0576

NATIONAL ASSEMBLY OF PEOPLE'S POWER

GOC-2022-832-O90

JUAN ESTEBAN LAZO HERNÁNDEZ, President of the National Assembly of People's Power of the Republic of Cuba.

I HEREBY INFORM: That the National Assembly of People's Power, in the session held on May 14, 2022, corresponding to the Fifth Extraordinary Period of Sessions of the Ninth Legislature, has approved the following:

WHEREAS: The Constitution of the Republic, in its Article 40, establishes that human dignity is the supreme value that sustains the recognition and exercise of the rights and duties enshrined therein, and in its Article 48 that all persons have the right to respect for their personal and family privacy, their own image and voice, their honor and personal identity.

WHEREAS: The Constitution, in its Article 97, recognizes the right of all persons to access their personal data in records, files or other databases and information of a public nature, as well as to request their non-disclosure and to obtain their due correction, rectification, modification, updating or cancellation, and that the use and processing of such data be carried out in accordance with the provisions of the law.

WHEREAS: Technological advances, and especially the digital environment, impact the economic, political and social life of people, in particular, the enjoyment of their rights, which is manifested in our society.

WHEREAS: The existence of registries, files, databases or other means of a public or private, physical or digital nature, through which personal information is stored, processed, provided and used, as well as the free access to such data, may violate the right of its owner and other rights to which it is related, if not adequately regulated.

WHEREAS: It is necessary to approve a regulatory provision that guarantees the right of individuals to the protection of their personal data, that regulates the use and processing of such data by public and private persons or entities, as well as information

ISSN 1682-7511

of a public nature, and that contributes to promote, foster and disseminate a culture of data protection in society.

WHEREFORE: The National Assembly of People's Power, in the exercise of the powers conferred upon it by Article 108 (c) of the Constitution of the Republic, has adopted the following:

LAW No. 149
OF PERSONAL DATA PROTECTION

CHAPTER I
GENERAL PROVISIONS

SECTION ONE
Preliminary provisions

The purpose of this Law is the following:

a) To establish the fundamental principles, procedures and definitions to guarantee the natural person the right to the protection of his personal data contained in registers, files, archives, databases or other technical means of data processing, whether physical or digital, of a public or private nature;
b) ensure due respect for personal and family privacy, self-image and voice, honor and personal identity;
c) regulate the use and effective treatment of personal data and public information by the persons or public and private entities responsible for or in charge of them; and
d) contribute to promoting, fostering and disseminating a culture of protection in society.

Article 2. The subjects of application of this Law are natural persons with respect to their data, and legal entities and natural persons, with respect to the processing of personal data they carry out.

Article 3.1. Personal data shall be considered to be information concerning a person or a group of persons.

The natural, identified or identifiable person, which can lead to their identity.

2. A person is identifiable when his or her identity can be determined directly or indirectly through any information.

Article 4. Personal data related to sex, age, image, voice, gender, identity, gender identity, sexual orientation, skin color, ethnic, national and territorial origin, migratory condition and classification, disability status, religious beliefs, political affiliation, marital status, domicile, medical or health, economic-financial, academic and training, professional and employment, judicial and administrative data, and any information related to these data that may lead to the identification of a given person, collected from registers, files, archives and databases, are protected.

Article 5. A register, file, archive and database shall be considered, indistinctly, the organized set of personal data that are the object of treatment or processing, electronic or otherwise, regardless of the modality of their formation, storage, organization and access.

Article 6. The processing of personal data consists of the systematic operations and procedures, whether electronic or not, that allow the collection, conservation, ordering, storage, modification, relation, evaluation, blocking, destruction and, in general, the processing of personal data, as well as its transfer to third parties through communications, consultations, interconnections and transfers.

Article 7.1. A responsible person is the natural or legal person, whether public or private, who decides on the purpose, content and use during the processing of personal data.

2. The person in charge is the natural or legal person, of a public or private nature, who individually or jointly with others, carries out the processing of personal data at the request of the data controller.

Article 8.1. The right to the protection of personal data is governed by the provisions of the Constitution, this Law and other regulatory provisions issued for this purpose by the competent bodies.

2. The limits to this right only apply to the rights of others, collective security, general welfare, respect for public order, the Constitution and the laws.

Article 9. In the processing of personal data of minors, the best interests of such minors shall prevail in all cases, in accordance with the applicable regulatory provisions and the international treaties in force to which the Republic of Cuba is a party.

SECOND SECTION

Personal data protection principles

Article 10. The protection and processing of personal data is governed by the following principles:

a) Collection limitation: the collection and storage of information that may lead to the identification of a specific person must be limited to what is relevant and strictly necessary for the purpose required, adjusted to a specific, lawful and explicit objective, and kept only for the time required for that purpose;
b) data quality: the personal data obtained, stored and processed must be truthful, accurate, complete, correct and updated, provided by the owner himself, without using unfair or fraudulent means to obtain it, and will remain so until the owner expresses and proves the need for its rectification, modification, updating or cancellation;
c) specification of the purposes: the specific purposes for the collection, storage and technical processing of any nature of personal data must be made known in advance to the holder accurately, in an understandable and relevant manner;
d) limitation of use: the personal data obtained, stored and processed may only be used for the specific and lawful purpose for which the owner was informed, and by natural or legal persons, or other entities authorized by the owner;
e) legitimacy: only bodies, agencies, entities and natural or legal persons are legitimized to obtain, store and process personal data when they have authorization for the formation of files, in accordance with their functions or the activities they perform, as regulated in the legislation in force for such purposes;
f) safeguarding security: natural or legal persons responsible for files containing personal data are obliged to safeguard their security and to guarantee, with the corresponding technological, administrative, material or physical measures, that only they or authorized personnel, as the case may be, access or process them according to the established procedures;
g) transparency of information: the person responsible and in charge of the personal data files guarantees the holder the exercise of his or her right of access.

The files must also be available for inspection or review by a competent authority;

h) individual participation: personal data can only be obtained with the individual participation of its owner, as an expression of respect for his or her right to identity, privacy, honor, image and voice;

i) Responsibility: the natural or legal persons in charge of obtaining, storing and processing personal data in registers, files, archives and databases are responsible for their lawful use for the purposes informed to their owner, guaranteeing their security;

j) legality: the possession and processing of personal data is exclusively for lawful purposes; the persons responsible for registers, files, archives and databases comply in their actions with the provisions of the corresponding regulatory provisions;

k) degrees of confidentiality of information: personal data provided to registries, files, archives and databases are confidential and may only be accessed by their owner or by a person with a proven legitimate interest.

l) consent: the owner must express his or her free, unequivocal, specific and informed will for the processing of personal data, specifying the purpose for which consent is given.

THIRD SECTION

Consent and sensitive personal data

Article 11.1. The person who processes personal data must have the consent of the data subject, except in the cases of exception provided for in this Law.

2. Consent may be express when it is expressed verbally, in writing or by any comparable means; or tacit when, having made available to the owner the purposes of the processing of his data, he does not express his will to the contrary.

Article 12. In any case, the owner must be informed, in an understandable and pertinent manner, of the lawfulness and specific purpose of the data requested, and has the right to know the recipients or class of recipients of such data, the optional or compulsory nature of providing them, where they are stored, what processing they may be subject to, the consequences of providing or not providing them and of their inaccuracy, as well as their storage regime.

Article 13.1. Consent for the collection, storage and processing of personal data of minors is given by them in accordance with their progressive autonomy, or by their fathers, mothers or legal representatives.

2. In the event of conflicting interests between the right holder and his representatives. The intervention of the public prosecutor is required.

Article 14.1. Persons with disabilities themselves give their consent to the collection, storage and processing of personal data pertaining to them, in appropriate cases assisted by the supports required in the exercise of their legal capacity, and use the appropriate personal and technical means.

2. When they have been appointed an intense support with powers of representation, it is up to this person to give consent in accordance with the wishes and preferences of the person with disabilities.

Article 15.1. Sensitive data is personal information whose unlawful use may give rise to discrimination, imply a distinction detrimental to human dignity or entail a serious risk for its owner.

Sensitive data are considered, among others, those that may reveal sex, gender, identity, gender identity, sexual orientation, ethnic origin and skin color, present or future health status, disability status, genetic information, or obtained from diagnostic tests performed in health institutions or linked to assisted reproduction techniques, religious beliefs, political affiliation, police and criminal records.

Article 16.1. A person may not be compelled to provide sensitive personal data, nor is its processing lawful without the express, unequivocal, free and informed consent of its owner, except in those cases of exception provided for in this Law.

2. The provisions of the preceding section are also applicable in the case of deceased persons, for which purpose the consent granted during their lifetime must be taken into account, if there is a statement to that effect in the will or declaration of will for that purpose; otherwise, the consent of their heirs or successors in title must be taken into account.

Article 17. Personal data may be obtained, stored and subjected to specific processing, without the express consent of the owner, only in the following cases:

a) By provision of law, provided that the principles stated herein are complied with;
b) by order or resolution of the prosecutor or the court;
c) in the face of an event that could potentially harm an individual's person or property;
d) if they are necessary for the purpose of preventive treatment, diagnosis or the provision of urgent health care;
e) if they are found in publicly accessible sources, provided that no principle for the protection of personal data, provided by this Law, has been violated;
f) if they are subjected to a prior procedure of data dissociation, understood as the processing of personal data in such a way that the information obtained cannot be associated with a specific or identifiable person;
g) if the owner of the personal data is reported missing; and
h) for reasons of general welfare, public order and in the interest of national defense and security.

Article 18.1. The provisions of the preceding articles do not exempt persons from the obligation to identify themselves before the corresponding authorities, in accordance with the legislation in force, which implies providing their identity data by means of the documents that accredit it.

2. The corresponding authorities should not require any information other than that reflected in such documents, in accordance with the provisions of Article 16, paragraph 1, of this Law.

CHAPTER II
HOLDER'S RIGHTS AND THEIR EXERCISE

SECTION ONE
Rights of individuals regarding their personal data

Individuals are holders of their personal data and have the right to non-disclosure of such data and, consequently, to respect for their personal and family privacy, their honor and personal identity, their own image and voice.

The owner has the right at all times to access his personal data and information of a public nature contained in registers, files, archives and databases or other technical means of data processing, whether physical or digital, public or private, and to know the information related to the conditions and generalities of their processing.

Article 21.1. The holder has the right to rectification, correction, modification and updating of his personal data by the person responsible or in charge of the registry, file, archive and physical or digital database, or other technical means of data processing, when they are inaccurate, incomplete or outdated.

2. Failure to comply with the obligation of proper collection, custody and use of the data, as well as the obstruction or denial of access to the owner of the personal data, generates liability and allows the owner to demand compensation for damages or losses caused, in accordance with the legislation in force.

The owner has the right to the cancellation of his personal data contained in registers, files, archives and databases, physical or digital, or other technical means of data processing, when he considers that the purpose for which they were obtained has been fulfilled or that the data is improperly processed, which affects or may significantly affect his interests and rights.

Article 23.1. The owner may object to the processing of his personal data when it may cause him harm or damage, or significantly affect his rights or legitimate interests.

2. He may also object to the processing of his personal data, whether automated or not, if it significantly harms his interests and rights, and is intended to evaluate certain personal aspects of the holder, analyze or predict, in particular, his professional performance, economic situation, state of health, reliability, behavior or entails a serious risk to the holder, as provided for in Article 15 of this Law, or any other that involves a distinction detrimental to human dignity.

SECOND SECTION
Exercising the rights of individuals over their personal data

Article 24.1. The holder, his legal representative or support, may exercise the rights of access, non-disclosure, rectification, correction, modification, updating, cancellation and opposition of the personal data concerning him, without being subject to an order of priority among these and in accordance with the provisions of this Law.

2. The owner, his legal representative or support, when requesting the rectification, correction, modification or updating of the data, attach the means of evidence that prove the requested action, since the data recorded is presumed to be true.

3. The exercise of these rights is subject to the procedures and deadlines established in this regulatory body and other provisions applicable to the matter.

Article 25.1. Requests to exercise the rights referred to in the preceding article are submitted by the owner, his legal representative or support, to the person responsible or in charge of the data processing, who within five working days decides whether or not they are admissible.

2. If the request referred to in the preceding articles is admissible, the responsible person shall make it effective within ten working days following the date on which the request was made.

3. The aforementioned terms may be extended once for an equal period of time. when justified by the circumstances of the case.

When the person responsible or in charge is not competent to deal with the request, he/she shall inform the owner of the situation within five working days following the filing of the request and shall direct him/her to the person who is competent to do so.

Article 27. Access to personal data information is fulfilled when the requested information is made available to the holder by means of the issuance of simple copies, electronic documents, exhibition of the data or any other direct and secure means.

Article 28.1. Access to personal data and its non-disclosure, or the correction, rectification, modification, updating, cancellation or opposition to the processing thereof, may be denied or refused in the following cases:

a) The database does not contain the applicant's personal data of interest;
b) the applicant is not the owner of the personal data, or the legal representative is not the owner of the personal data, or the legal representative is not the owner of the personal data.
duly accredited for this purpose;
c) the rights of a third party are infringed;
d) there is a final decision of a competent court that restricts access to personal data, or does not allow the rectification, cancellation or opposition of such data;
e) rectification, correction, modification, updating, cancellation or opposition. has been previously carried out;
f) for reasons of general welfare, public order and in the interest of national defense and security;
g) others that significantly so warrant; and
h) when the registry in which the personal data is recorded is covered by established regulations limiting access to such information.

2. In the above cases the person responsible or in charge decides, by means of a reasoned resolution, which notifies the owner of the data or, as the case may be, his legal representative or support, within the established deadlines.

THIRD SECTION

On the action for the protection of personal data

Article 29. The owner of personal data, within ten working days, may establish the action for the protection of personal data against the person responsible or in charge of a public or private registry, file, archive or database, when:

a) When requesting access to personal data or information of a public nature contained in a registry, file, archive, database or similar and such information has been denied, or has not been provided by the person responsible or in charge of the database within the opportunities and deadlines provided by law; and

b) has requested, to whoever is responsible or in charge of the registry, file, archive, database or treatment, its non-disclosure, rectification, correction, modification, updating, cancellation or opposition, and the latter has not proceeded to do so or given sufficient reasons why what was requested does not correspond, or what has been resolved does not satisfy the claim, within the term provided for such purpose by law.

Article 30.1. The hierarchical superior of the persons responsible for or in charge of the database, when they are in an organ, agency of the Central Administration of the State and national entities, or their dependencies, are competent to hear in the first instance the actions for the protection of personal data.

2. In the event that the person responsible or in charge is a natural person or if such databases are not located in an organ, agency of the Central Administration of the State and national entities or their dependencies, the action for protection of personal data is filed before the competent court.

The affected owner himself, his legal representative or support and, in the case of deceased persons, his heirs or successors in title, shall be entitled to bring an action in accordance with Article 29.

Article 32.1. For an action for the protection of personal data brought pursuant to Article 30(1), the parties shall be summoned to a hearing within ten working days from the date of the filing of the complaint.

2. To this end, the claim is sent to the defendant no less than three working days prior to the act indicated, unless the action is manifestly inadmissible, in which case the authority that must resolve it rejects it without processing it and files the proceedings, informing the claimant.

3. At the hearing, the parties are heard, the evidence provided by the parties is received, and any necessary evidence is taken.

4. At any time, the authority may order ex officio proceedings by the authority that must be resolved.

Article 33. The claim of the personal data protection action referred to in the preceding article is settled by means of a resolution issued within five working days following the holding of the hearing; in exceptional cases it may be extended for the same period and the decision is immediately notified to the interested parties, leaving a record in the file that is formed for such purposes.

The resolution declaring the action for the protection of personal data admissible shall contain:

a) The specific identification of the authority or person to whom it is addressed and against whom it is directed.
   action, fact or omission the claim is granted;
b) the precise determination of what is to be done or not to be done and the period of time for which it is to be done.
   resolution shall govern, if it is appropriate to fix it; and
c) the term for compliance with the provisions, which is set by the person who resolves according to the circumstances of each case, and shall not be longer than fifteen consecutive and uninterrupted business days, computed as of the notification.

Article 35.1. If, in the judgment of the decision-maker, the need for immediate action is apparent, prior to the definitive solution of the case and on a provisional basis, the measures required to safeguard the right allegedly violated may be ordered.

2. The provisions of the preceding paragraph may be disposed of by the person who resolves at any time during the process, as the case may be.

A lawsuit may be filed before the competent court against the decision in the action for the protection of personal data.

The action for the protection of personal data brought pursuant to Article 30, paragraph 2, shall be governed by the rules and procedures contained in the procedural law in force.

Article 38.1. No preliminary questions, counterclaims or motions may be raised in the proceedings for the protection of personal data.

2. The authority, at the request of a party or ex officio, remedies procedural defects, ensuring, within the summary nature of the process, the validity of the counter-dictatorial principle.

SECTION FOUR

The regime for the conservation of personal data

Article 39.1. The regime for the conservation of personal data shall be in accordance with the provisions applicable to the matter in question and shall take into account legal, administrative, historical or other aspects.

2. The storage regime may not exceed the time limits for the fulfillment of the purposes justifying its processing.

3. Personal data that have fulfilled the purposes for which they were processed in accordance with the applicable provisions are deleted, ex officio or at the request of the owner of the registers, files, archives and physical or digital databases, or other technical means of data processing in which they are kept, once the retention period has expired.

4. The conservation regime is up to five years, provided that a different term is not established by law or the owner consents to another term.

CHAPTER III

OF THE TREATMENT OF PERSONAL DATA

SECTION ONE

Control of personal databases

The registry, file, archive or database, both public and private, which by virtue of the purpose for which they have been created are of public interest, are controlled at the national level, as well as others determined by the authorized authority at the proposal of the organs, agencies of the Central Administration of the State and national entities or their dependencies, which contain personal data.

Article 41. The national control of registry, file, archive or personal data bases collects the following information:

a) Name and surname, identity card and legal address of the natural person authorized to provide services, responsible for the collection of the data; in the case of the legal person, the data that identifies it;
b) characteristics and purpose of the records, files, archives, databases or other physical or digital media and information collected;
c) personal data that make up the content of records, files, archives, databases or other physical or digital media;
d) data collection and updating methods;
e) location and destination of the data;
f) means used to ensure data security;
g) assignments, interconnections or transfers foreseen;

h) identification of persons with access to information processing;
i) data retention time; and
j) form and conditions under which persons with legitimate interest may access the data collected, procedures for rectification, correction, modification, updating, cancellation or opposition of the data.

Article 42. Natural and legal persons that have a registry, file, archive or personal data bases in accordance with the provisions of this Law, declare their existence before the authorized authority and notify the latter of any changes in the information recorded, which guarantees transparency and legal security of these databases before third parties.

Article 43. Failure to comply with the provisions of the preceding article may result in the application of the sanction and measures provided for in this Law.

SECOND SECTION

Obligations in the processing of personal data

Article 44.1. The person responsible or in charge of the processing of personal data guarantees the material, technical and organizational conditions to follow up on the requests of the holders in the exercise of their rights; adopts measures for the security of the data and prevents its alteration, loss, unauthorized processing or access; likewise, promotes communication and legal education actions on the protection of personal data.

2. In no case does it process personal data of a nature other than the stated purposes.

The person who, in the exercise of legally authorized functions, has access to the data, is obliged to observe the due reserve and confidentiality that this requires, to which end the data controller notifies him/her of the responsibility he/she acquires and the legal consequences of non-compliance.

In cases of cancellation of personal data, the person responsible for or in charge of the same establishes the destination to be given to the same or the measures to be adopted for their destruction.

Article 47. Legal or natural persons that provide services involving the processing of personal data in their registers, files, archives or databases, are obliged to protect such data and to inform about it at the time it is obtained, either directly or during registration on websites and computer applications, by means of a privacy notice, in compliance with the requirements set forth in Article 12 of this Law.

The person responsible for or in charge of the processing of records, files, archives or personal databases is obliged to notify the competent authority of the occurrence of cybersecurity incidents, in accordance with the provisions of the legislation in force.

THIRD SECTION

Processing of personal data from of images and voice obtained through the use of video protection cameras or any other device

Article 49.1. Personal data such as image and voice, when captured by video cameras or any other device that allows their recording in premises, dwellings and facilities and spaces where services of public interest are provided, may in no case cause an injury to the rights and guarantees recognized in the Constitution and this Law.

2. The installation of the devices mentioned in the previous paragraph is justified only if the purpose is legitimate, provided that no other means can be used.

3. The improper use and processing of personal data from images and voice obtained through the use of video protection cameras or any other device, may give rise to an action for the protection of personal data, as well as the corresponding civil or criminal liability.

Article 50. Natural or juridical persons that provide services of public interest are obliged to inform of the presence of these media and to place identifiers in the areas where they are located.

Article 51. The means of image and voice collection installed in private spaces may not include their collection in public spaces, unless it is indispensable or impossible to avoid in accordance with their location, complying with the obligation described in the preceding article.

Article 52. Image and voice recordings obtained by this means cannot be used for purposes other than those for which they were intended.

The treatment of image and voice recordings from video protection cameras related to the armed institutions of the State comply with the principles declared in the present Law, and their treatment is regulated in accordance with the rules issued by the competent authorities.

The use of recordings of images and voice of persons obtained from mobile telephones, photographic cameras, tape recorders or other similar devices may in no case affect the rights protected in Article 19 of this Law. Article 55.1. The mass media, in any of their manifestations and supports, in the processing of personal data, including image and voice recordings, comply with the principles stated herein and ensure that they comply with the provisions of this Law.

in Article 19.

2. Informed consent is not required for these purposes in the case of persons of recognized patriotic, revolutionary, leadership, scientific, teaching, cultural, sports, service to the people, personalities, public officials in the exercise of their functions, or in the case of a person who is not the focus of the information or when such information is of a public nature.

SECTION FOUR

Non-compliance with provisions relating to the protection of personal data

Article 56.1. Natural or legal persons subject to the legal regime established by this Law, who fail to comply with the provisions relating to the protection of personal data, shall be imposed by the competent authority the following sanctions and measures:

a) Warning;
b) fine of up to 20,000 pesos;
c) suspension of the respective database for a period of up to five days; and
d) closure of the registry, file, archive or database.

2. These sanctions and measures are graduated taking into account the social impact, seriousness, repetition or recidivism of the infraction committed.

3. Sanctions and measures are applied without prejudice to any civil or criminal liability that may be incurred.

4. The competent authority to impose the fine and other measures corresponding to non-compliance with the provisions related to the protection of personal data, are the officials expressly authorized by the bodies, agencies of the Central State Administration and national entities, within the scope of their competence.

Article 57.1. Against the sanction or measure imposed by the competent authority, the affected party may file an appeal in writing within ten working days following the date of notification.

2. The immediate superior of the authority that imposed the sanction or measure is empowered to hear and resolve the appeal.

3. In the appeal filed, the appellant proposes the following evidence
that it intends to avail itself of for the purposes of its challenge.

Article 58. The immediate superior who hears the appeal may summon the appellant to be heard on his challenge.

The appeal does not interrupt the execution of the sanction or measure imposed.

Article 60.1. The appeal shall be resolved within a period of up to ten working days following its filing.

2. Said term may be extended for an additional ten working days, if the evidence presented makes it necessary.

3. The appellant is notified of the decision resolving the appeal within
within three working days from the date of its issuance.

In the event that the appeal is declared admissible, the decision shall be communicated to those who have intervened in the execution of the sanction or measure.

Article 62. The decision of the authorized administrative authority may be challenged in a judicial proceeding.

SECTION FIVE

National and international transfer of personal data

The transfer of personal data within the national territory is authorized, at the request of the data controllers or data processors, in the following cases:

a) Exchange of medical, health or research data when required for the treatment of the owner or in the collective interest;
b) when the purpose of the data transfer is for the general welfare, the order of the country, the
public and national defense and security interests;
c) bank transfers with respect to the respective transactions;
d) to facilitate the exercise of the right to vote in terms of voter registration; and
e) for other significant reasons.

Article 64. The persons responsible for or in charge of processing personal data are responsible for authorizing the transfer thereof within the scope of their competencies, in compliance with the principles set forth in this Law.

Article 65.1. The international transfer of data, at the request of the responsible authority of the receiving country, proceeds in the following cases:

a) International judicial collaboration;
b) exchange of medical data when required for the treatment of the data subject, and epidemiological research, as long as it is carried out after the adoption of a procedure of dissociation of the information, with the purpose of making the data subject unidentifiable;
c) bank or stock exchange transfers with respect to the respective transactions and in accordance with applicable law;
d) when the transfer has been agreed within the framework of international treaties to which the Republic of Cuba is a party; and
e) when the transfer of data is for the purpose of international inter-agency cooperation in the fight against organized crime, terrorism, money laundering, drug trafficking and other crimes subject to such cooperation.

2. To authorize the international transfer of data, account is taken of the nature of the data requested, the purposes for which they are used, the consent of or information to the data subjects in the cases required, the duration of the processing to which they are subjected or which are foreseen, the country of origin and final destination of the information, applicable general or special rules of law, specific professional rules applicable and technical and organizational security measures in force in the destination countries.

The President of the People's Supreme Court, the Attorney General of the Republic, the Minister-President of the Central Bank of Cuba and the Ministers of Foreign Affairs, the Interior, Justice and Public Health are empowered to authorize the international transfer of personal data within the scope of their competencies.

SPECIAL PROVISIONS

FIRST: The Minister of Justice, within a term of up to one (1) year from the effective date of this Law, creates the national control of registries, files, archives or personal data bases, for which he/she is responsible and over which he/she exercises the maximum supervision.

SECOND: Those responsible or in charge of the registers, files, archives or personal data bases declare, within a period of up to one (1) year from the creation of the national control, the existence of these.

FINAL PROVISIONS

FIRST: To entrust the Ministry of Justice with the control of compliance with the provisions of this Law.

SECOND: The Council of Ministers, on an exceptional basis, authorizes the international transfer of personal data in cases not provided for in this Law, at the proposal of the Head of the corresponding organ, agency of the Central State Administration or national entity.

THIRD: The Ministers of the Revolutionary Armed Forces and of the Interior shall apply the provisions of this Law, in accordance with the characteristics of their agencies, and shall adopt the measures to modify, adapt or dictate the corresponding regulations.

FOURTH: The heads of the organs, agencies of the Central Administration of the State and national entities shall establish the corresponding internal regulations to adopt the necessary measures to comply with the provisions herein.

FIFTH: This Law shall enter into force one hundred and eighty (180) days after its publication in the Official Gazette of the Republic of Cuba.

BE IT PUBLISHED in the Official Gazette of the Republic of Cuba.

GIVEN in the Session Room of the National Assembly of People's Power, Convention Palace, in Havana, on the 14th day of the month of May, 2022.

Juan Esteban Lazo Hernández
President of the National Assembly
of the People's Power

Miguel Mario Diaz-Canel Bermudez
President of the Republic of Cuba

MINISTRY

COMMUNICATIONS

GOC-2022-833-O90

RESOLUTION 58/2022

WHEREAS: Law 149 "On Personal Data Protection", of May 14, 2022, establishes the fundamental principles, procedures and definitions to guarantee the natural person the right to the protection of his personal data contained in registers, files, archives, databases or other technical means of data processing, whether physical or digital, public or private.

WHEREAS: The advancement of the computerization process of society and the increase in the automated processing of personal data in the country make it necessary to complement the legislation in force regarding the security of Information and Communication Technologies, with a regulation that regulates the security requirements in the processing of personal data in electronic support.

WHEREFORE: In exercise of the powers conferred by Article 145, subsection d), of the Constitution of the Republic of Cuba, in connection with Article 24, subsection I), numeral 1, of the Sole Annex of Resolution 1, of August 7, 2017, of the Council of Ministers,

RESOLVED

SOLE: Approve the following:

REGULATION FOR THE SAFETY AND SECURITY OF PERSONAL DATA IN ELECTRONIC FORMAT

The purpose of these Regulations is to establish the requirements for the security and protection of personal data in electronic format.

This Regulation is applicable to operators and providers of public telecommunications and information and communication technology services, to

The following shall be excluded from the scope of this article: hosting and lodging companies, application companies and owners of private networks, as well as those who carry out activities related to the processing of personal data in electronic format, hereinafter referred to as those responsible for and in charge of registers, files, archives and databases.

Pursuant to the provisions of Law 149 "On the Protection of Personal Data", the processing of personal data in electronic support is considered to be the systematic operations and procedures that allow the collection, conservation, organization, storage, modification, relation, evaluation, blocking, destruction and, in general, the processing of personal data, as well as its transfer to third parties through communications, consultations, interconnections and transfers, when carried out through the use of telecommunications and Information and Communication Technologies.

Article 4. The persons responsible for and in charge of registers, files, archives and databases of

data must:

a) To ensure the security and protection of personal data in electronic format as part of the provision of its services;
b) establish the necessary technical and administrative measures to guarantee the processing of personal data in electronic format, in accordance with the provisions of this Regulation and other regulations in force; and
c) notify the competent authorities of the occurrence of cyber security incidents involving personal data on electronic media in their custody.

The persons responsible for and in charge of registers, files, archives and databases are the only ones authorized to manage computer programs or applications related to databases containing personal data in electronic format.

Article 6. The persons responsible for the registry, file, archive and database shall have the following duties and responsibilities

following obligations:

a) Create ways for the owner of the personal data in electronic format, his support or legal representative to access, modify and cancel them at the time he/she so determines, as soon as possible and with the greatest possible transparency;
b) establish the cancellation of personal data in electronic format at the request of the owner, his support or legal representative or when the purpose for which it was collected has been fulfilled, provided that it does not violate the provisions of a specific law or that it needs to be kept for legal, administrative, historical or other reasons, and adopt the necessary technical measures for the deletion of any link to this data and copies;
c) define the terms and conditions regarding the use of personal data in electronic support, which must be understandable by any user and establish the ways for the user to confirm his approval in accordance with the characteristics of the database and the service;
d) maintaining the confidentiality and integrity of personal data in electronic format and preventing their unauthorized access, modification or transfer; and
e) guarantee the backup of personal data on electronic media.

Article 7. The persons in charge and those in charge may only host or replicate records, files, archives and databases on electronic media that contain

personal data in national servers located in the country, except as provided by law.

Article 8. The terms and conditions of use of the service are applied in accordance with the provisions of Law 149 "On Personal Data Protection" and the characteristics of the database and the service in particular, and include the following aspects:

a) Inform the user the purpose of the collection of personal data at the time of his request, where they are stored and the period of time for which they are retained to fulfill its purpose;
b) describe the options that allow the data subject to manage his or her privacy;
c) alert the user about the use of elements on the website that can be used to track their activity, such as cookies, even if they are applied by third parties;
d) communicate to the user at least 3 months in advance any modifications to the text of the terms and conditions, by e-mail, SMS, notification in the software and computer application, website or other means; and
e) establish the minimum term for the cancellation of personal data in electronic format, which must not be longer than the provisions of the legislation in force on the matter.

Article 9.1. Personal data in electronic format may be used for academic, research or social purposes, with data analysis techniques, provided that they are anonymized or dissociated and their collection includes only the minimum data necessary to fulfill their purpose.

2. The exchange of information for the realization of these objectives must be carried out in a contractual manner between the person responsible for the database and the person using the data, and comply with the provisions of this Resolution.

3. The exchange of anonymized or anonymized data with another entity for use for the purposes expressed in paragraph 1 of this article, is carried out without commercial interest.

Article 10. The holders of personal data in electronic support who are users of public telecommunications services, computer programs and applications, and of social networks and Internet services offered by national entities, have the following rights:

a) Know the purpose for which your data is requested and the use to which it is put;
b) access, update and cancel, at the time they deem appropriate, the personal data provided for the use of the service;
c) that their data be cancelled when they deem it convenient, when the purpose for which it was collected has been fulfilled or when they consider that it is being processed in a way that violates their interests and rights; and
d) be informed about the available privacy settings options that are available to them. allow them to determine how their information is treated, shared and stored.

FINAL PROVISIONS

FIRST: The General Directorate of Information Technology, the Inspection Directorate and the territorial Control Offices of the Ministry of Communications shall be in charge, as appropriate, of controlling compliance with the provisions of this Resolution.

SECOND: This Resolution enters into force 180 days after its publication.
publication in the Official Gazette of the Republic of Cuba.

NOTIFY the General Director of Informatics, the Director of Inspection and the territorial directors of Control of the Ministry of Communications.

COMMUNICATE to the Vice Ministers, the Director General of Communications, the Director of Regulations, all of the Ministry of Communications.

BE IT PUBLISHED in the Official Gazette of the Republic of Cuba.

FILE the original at the Legal Department of the Ministry of Communications. DONE at Havana, on the 19th day of the month of August, 2022.

Wilfredo González Vidal
First Deputy Minister