

LEGISLATIVE ASSEMBLY OF THE REPUBLIC OF COSTA RICA

**PROTECTION OF THE PERSON IN
PERSONAL DATA PROCESSING**

FINAL LANGUAGE

March 21, 2011

FILE No. 16,679

**SECOND LEGISLATURE
(From May 1, 2010 to April 30, 2011)**

**SECOND PERIOD OF EXTRAORDINARY SESSIONS
(From December 1, 2010, to April 30, 2011)**

**DEPARTMENT OF LEGISLATIVE COMMISSIONS
SPECIAL PERMANENT DRAFTING COMMISSION**

THE LEGISLATIVE ASSEMBLY OF THE REPUBLIC OF COSTA RICA

DECREES:**PROTECTION OF THE PERSON IN
PERSONAL DATA PROCESSING****CHAPTER I
GENERAL PROVISIONS
SOLE SECTION****ARTICLE 1.- Objective and purpose**

This law is a public policy, and its objective is to guarantee to any person, regardless of nationality, residence or domicile, the respect of his fundamental rights, concretely, his right to self-determination in information concerning his life or private activity and other privacy rights, as well as defense of his freedom and equality concerning the automated or manual processing of the data concerning his person or assets.

ARTICLE 2.- Scope of application

This law will apply to personal data appearing in automated or manual databases or public or private entities and to any modality of subsequent use of these data.

The system of personal data protection established in this law will not apply to databases kept by physical or legal persons exclusively for internal, personal or household purposes, provided they are not sold or otherwise marketed.

ARTICLE 3.- Definitions

For the purposes of this law, the following are defined:

- a) Database: any archive, file, record or other structured set of personal data that is the object of treatment or processing, automated or manual, regardless of the modality of its preparation, organization or access.
- b) Personal data: any data concerning an identified or identifiable physical person.

- c) Unrestricted access personal data: those contained in public databases with general access, according to special laws and pursuant to the purpose for which such data are collected.
- d) Restricted access personal data: those that, even though they are part of public access records, do not have unrestricted access, because they are of interest only to the data subject or the Public Administration.
- e) Sensitive data: information concerning the intimate realm of the person, such as, for example, those that reveal racial origin, political opinions, religious or spiritual convictions, socioeconomic condition, biomedical or genetic information, sexual life and orientation, inter alia.
- f) Confidentiality duty: obligation of the data controllers, their personnel and the personnel of the Agency for the Protection of the Data of the Inhabitants (Prodhav) to keep confidentiality in the exercise of the powers given by this law, mainly when accessing information on personal and sensitive data. This obligation will survive even after the end of the relationship with the database.
- g) Data subject: physical person, holder of the data subject to automated or manual processing.
- h) Data controller: physical or legal person who administers, manages or is in charge of the database, be it a public or private entity, competent pursuant to the law to decide the purpose of the database, the categories of personal data that must be recorded and the type of processing to be applied to them.
- i) Personal data processing: any operation or set of operations done by automated or manual procedures and applied to personal data, such as collection, registration, organization, preservation, modification, extraction, consultation, use, communication by transmission, broadcast or any other form that facilitates access to them, comparison or interconnection, as well as their blockage, elimination or destruction, inter alia.

CHAPTER II

PRINCIPLES AND RIGHTS FOR PERSONAL DATA PROTECTION

SECTION I

BASIC PRINCIPLES AND RIGHTS

ARTICLE 4.- Self determination in information

Any person has the right to self determination in information, which covers all principles and guarantees related to the legitimate processing of their personal data recognized in this section.

The self determination in information is also recognized as a fundamental right in order to control the flow of information concerning each person arising from the right to privacy, avoiding the occurrence of discriminatory actions.

ARTICLE 5.- Principle of informed consent**1.- Obligation to inform**

When personal data are requested, it will be necessary to first inform the data subjects or their representatives, in an express, precise and unequivocal manner:

- a) Of the existence of a database of personal data.
- b) Of the purposes pursued by collecting these data.
- c) Of the addressees of the information as well as those who can consult it.
- d) The mandatory or optional character of their answers to the questions asked of them during data collection.
- e) Of the processing given to the data requested.
- f) Of the consequences of the refusal to provide the data.
- g) Of the possibility to exercise their rights.
- h) Of the identity and address of the controller of the database.

When questionnaires or other means are used to collect personal data, these warnings must be clearly legible.

2.- Granting consent

The person who compiles personal data must obtain the express consent of the data subject or his representative. This consent must be in writing either in a physical or electronic document, which may be revoked in the same manner without retroactive effect.

Express consent will not be necessary when:

- a) There is a motivated order, rendered by a competent judicial authority or a decision made by a special investigation commission of the Legislative Assembly in the performance of its function.
- b) The personal data have unrestricted access, obtained from general public access sources.
- c) The data must be delivered by constitutional or legal provision.

It is prohibited to collect data without the informed consent of the person or acquire them by fraudulent, unfair or illegal means.

ARTICLE 6.- Principle of quality of the information

Personal data may be collected, stored or used for automated or manual processing only when the data are current, truthful, exact and adequate for the purpose for which they were collected.

1.- Current Character

The personal data must be current. The controller of the database will eliminate the data that are no longer pertinent or necessary for the purpose for which they were received and recorded. Personal data that may affect in any manner their subject will not be kept in any case after the lapse of ten years from the date of occurrence of the facts recorded, except if otherwise ordered by a special regulatory provision. If it is necessary to keep such data beyond the stipulated term, they must be disassociated from their subject.

2.- Truthfulness

The personal data must be truthful.

The controller of the database is obligated to modify or eliminate the data which are not truthful. Equally, he will make sure that the data are processed in a fair and legal manner.

3.- Exactness

The personal data must be exact. The controller of the database will take the necessary measures for the inexact or incomplete data concerning the purposes for which they were collected or for which they were subsequently processed, to be eliminated or corrected.

If the personal data recorded are inexact in full or in part or incomplete, they will be eliminated or replaced ex officio by the controller of the database, with the corresponding rectified,

updated or expanded data. Equally, they will be eliminated if there is no informed consent or if their collection is prohibited.

4.- Suitability for the purpose

The personal data will be compiled with certain, explicit and legitimate purposes, and will not be processed subsequently in a manner incompatible with such purposes.

The subsequent processing of data for historical, statistical or scientific purposes will not be deemed incompatible if the appropriate guarantees are established to protect the rights contemplated in this law.

The databases may not have purposes contrary to the laws or public morality.

ARTICLE 7.- Rights of the person

Each person has guaranteed right to access his personal data, to correct or eliminate them and to consent to the assignment of his data.

The controller of the database must comply with the request of the person free of charge and resolve in the appropriate sense within the term of five business days from the receipt of the request.

1.- Access to information

The information must be stored so as to fully guarantee the right of access of the data subject.

The right of access to personal information guarantees the following powers of the data subject:

- a) Obtain at reasonable intervals, as provided by regulation, without delay and free of charge, the confirmation or lack thereof concerning the existence of his data in archives or databases. If his data do exist, they must be communicated to the data subject in a precise, easy to understand manner.
- b) Receive information about his person, as well as the purpose for which it was compiled and the use given to his personal

- data. The report must be complete, clear and free of codes. It must be accompanied by an explanation of the technical terms used.
- c) Be informed in writing, extensively, by physical or electronic means on the entire record belonging to the data subject, even if the requests includes only one aspect of the personal data. This report may not reveal in any case data belonging to third parties, even if they are related to the data subject, except when they are required to prove a criminal offense.
 - d) Have knowledge, if applicable, of the system, program, method or process used in the processing of his personal data.

The exercise of the right referred to in this article, in the case of data of deceased persons, will belong to their successors or heirs.

2.- The right of rectification

The right to obtain, if applicable, the rectification of the personal data and their update or elimination when they were processed by violation of the provisions of this law is guaranteed, especially due to the incomplete or inexact character of the data, or because they were compiled without authorization from the data subject.

Any data subject may request and obtain from the controller of the database the rectification, update, cancellation or elimination and compliance with the confidentiality guarantee concerning their personal data.

The exercise of the right referred to in this article, in the case of data of deceased persons, will belong their successors or heirs.

ARTICLE 8.- Exceptions to the self-determination and information of the citizen

The principles, rights and guarantees established herein may be limited in a fair, reasonable manner according to the principle of administrative transparency, when the following purposes are pursued:

- a) The security of the State.
- b) The security and performance of public authority.
- c) The prevention, persecution, investigation, detention and repression of criminal offenses or professional ethics violations.
- d) The operation of databases used for statistical, historical or scientific investigation purposes when there is no risk for the persons to be identified.

- e) Adequate performance of public services.
- f) Efficient routine activity of the Administration, by official authorities.

SECTION II

SPECIAL DATA PROCESSING CATEGORIES

ARTICLE 9.- Special data categories

In addition to the general rules established in this law, for personal data processing, the special data categories to be mentioned below will be governed by the following provisions:

1.- Sensitive data

No person will be obligated to provide sensitive data. It is prohibited to process personal data that reveal the racial or ethnic origin, political opinions, religious, spiritual or philosophical convictions, as well as those concerning the health, sexual life and orientation, inter alia.

This prohibition will not apply when:

- a) The processing of the data is necessary to protect the vital interest of the data subject or another person in the event that the data subject is physically or legally incompetent to give consent.
- b) The processing of the data is done in the course of its legitimate activities and with due guarantees by a foundation, association or any other agency with political, philosophical, religious or union purposes, provided it refers exclusively to its members or the persons who keep regular contact with the foundation, association or agency, for reasons of its purpose and provided that the data are not communicated to third parties without the consent of the data subjects.
- c) The processing concerns data which the data subject has made voluntarily public or are necessary for the recognition, exercise or defense of a right in a lawsuit.

- d) The processing of the data is necessary for medical prevention or diagnosis, providing health assistance or medical treatments, management of health services, provided that the processing of the data is done by a healthcare clerk subject to professional secrecy or the secrecy typical for his function or by another person who is also subject to an equivalent secrecy obligation.

2.- Restricted access personal data

Restricted access personal data are those which, even though they are part of public access records, do not have unrestricted access because they are of interest only to their subject or to the Public Administration. Their processing will be permitted only for public purposes or in case of express consent of the data subject.

3.- Unrestricted access personal data

Unrestricted access personal data are those contained in public databases with general access as provided by special laws and according to the purpose for which the data were collected.

The following are not deemed included in this category: the exact residential address, except if its use is the product of a mandate, summons or administrative or court notice, or a bank or financial operation, photography, private telephone numbers and others of the same nature whose processing may affect the rights and interests of the data subject.

4.- Data concerning credit behavior

The data concerning credit behavior will be governed by the rules regulating the national financial system so as to allow guaranteeing an accessible degree of risk by the financial entities, without preventing the full exercise of the right to self determination in information or exceed the limits of this law.

SECTION III

SECURITY AND CONFIDENTIALITY OF DATA PROCESSING

ARTICLE 10.- Data security

The controller of the database must adopt the technical and organizational measures necessary to guarantee the security of personal data and avoid their alteration, accidental or illegal destruction, loss, unauthorized processing or access as well as any other action contrary to this law.

Said measures must include at least the most adequate physical and logical security mechanisms according to current technological development to guarantee the protection of the information stored.

Personal data will not be stored in databases that do not meet the conditions that fully guarantee their security and integrity as well as that of the processing centers, equipment, systems and programs.

By regulation, requisites and conditions will be established to be met by automated and manual databases and of the persons intervening in the collection, storage and use of the data.

ARTICLE 11.- Confidentiality duty

The controller and those who intervene in any phase of personal data processing will be obligated to keep professional or functional secrecy even after the end of their relation with the database. The controller may be relieved from the duty of secrecy by court decision as strictly necessary and within the case being heard.

ARTICLE 12.- Action protocols

The physical and legal, public and private persons whose functions include the collection, storage and use of personal data may issue an action protocol establishing the steps to be followed in the collection, storage and handling of personal data according to the rules provided in this law.

To be valid the action protocols must be recorded, as well as their subsequent modifications, with Prodhav. Prodhav may verify at any time that the database is fully complying with the terms of its protocol.

Data handling based on an action protocol registered with Prodhav will create the presumption, “juris tantum,” of compliance with the provisions

contained in this law, in order to authorize the assignment of the data contained in a base.

ARTICLE 13.- Effective guarantees

Any data subject has the right to simple and quick administrative proceeding with Prodhab in order to be protected against acts that violate his fundamental rights recognized by this law. The above is without prejudice to the general or specific jurisdictional guarantees established by law for the same purpose.

CHAPTER III

TRANSFER OF PERSONAL DATA

SOLE SECTION

ARTICLE 14.- Transfer of personal data, general rule

The controllers of public or private databases may transfer the data contained in them only when the data subject authorized such transfer expressly and validly, and it is done without impairing the principles and rights recognized in this law.

CHAPTER IV

AGENCY FOR THE PROTECTION OF THE DATA OF THE INHABITANTS
(Prodhab)

SECTION I

GENERAL PROVISIONS

ARTICLE 15.- Agency for the Protection of the Data of the Inhabitants (Prodhab)

A fully decentralized entity is created under the auspices of the Ministry of Justice and Peace, named Agency for the Protection of the Data of the inhabitants (Prodhab). It will have its own instrumental legal identity in the performance of the functions assigned to it by the law, in addition to the administration of its funds and budget and to sign the contracts and agreements it needs to perform its functions. The Agency will enjoy independence of opinion.

ARTICLE 16.- Functions

The functions of Prodhab, in addition to others imposed by this or other regulations, are as follows:

- a) Ensure compliance with the regulations in matters of data protection, both by private, physical or legal persons and by public entities and agencies.
- b) Keep a record of the databases governed by this law.
- c) Require the information necessary to perform its function from the administrator of databases, including the protocols used.
- d) Access the databases governed by this law, in order to effectively enforce the rules on personal data protection. This function will apply for the concrete cases presented to the Agency and, exceptionally, when there is evidence of generalized misuse of the database or information system.
- e) Resolve complaints for violations of the rules on the protection of personal data.
- f) Order, ex officio or upon request, the elimination, rectification, addition or restriction in the circulation of the information contained in files and databases, when they violate the rules on personal data protection.
- g) Impose the sanctions established in article 28 of this law on the physical or legal, public or private persons who violate the rules of personal data protection and forward those that may constitute a crime to the Prosecutor's Office.
- h) Promote and contribute to the writing of regulations to implement the rules on personal data protection.
- i) Issue the necessary guidelines, which must be published in the official newspaper, La Gaceta, so that public institutions may implement adequate procedures concerning personal data handling, respecting the various degrees of independent autonomy and functional independence.

- j) Support, among the inhabitants, the knowledge of the rights concerning the collection, storage, transfer and use of the personal data.

In the performance of its functions, Prodhab must use automated procedures, according to the best technological tools within its reach.

ARTICLE 17.- Management of the Agency

The Management of Prodhab will be entrusted to a national director, who must have at least the academic degree of bachelor in a matter related to the object of their function and have recognized professional and moral solvency.

The appointed national director may not be a person who is owner, shareholder, member of the board of directors, manager, advisor, legal representative or employee on a company engaging in the collection or storage of personal data. Such prohibition will persist for up to two years after their functions or corporate connection has stopped. Also prohibited are the spouses or relatives, up to the third degree of consanguinity or affinity, of a person who is any of the situations mentioned above.

ARTICLE 18.- Personnel of the Agency

Prodhab will have the technical and administrative personnel necessary for the good performance of its functions, designated by competition based on skills, according to the Civil Service Statute or as provided by regulations. The personnel will be obligated to keep professional secrecy and will have a duty of confidentiality concerning the personal data learned by them in the performance of their functions.

ARTICLE 19.- Prohibitions

All employees of Prodhab are subject to the following prohibitions:

- a) Render services to persons or companies engaging in the collection, storage or handling of personal data. Such prohibition will persist for up to two years after they left their functions.
- b) Obtain personal undue interest in matters known to the Agency.
- c) Reveal or otherwise disclose the personal data to which they had access in connection with their position. This prohibition will persist indefinitely, even after they have left their function.

- d) In the case of officials appointed in professional positions, practice their profession outside. The above has the exception of engaging in teaching activities in higher education institutions or liberal practice in favor of relatives by consanguinity or affinity up to the third degree, provided they do not fall into the situations in paragraph a).

Noncompliance with any of the above prohibitions will be deemed serious misdemeanor for the purposes of application of the disciplinary system, without prejudice to other forms of liability that such conducts may imply.

ARTICLE 20.- Budget

The budget of Prodhab will consist of the following:

- a) Royalties, rates and fees obtained in the performance of its functions.
- b) Transfers made by the State to the Agency.
- c) Donations and subsidies coming from other states, national public institutions or international agencies, provided they do not compromise the independence, transparency and autonomy of the Agency.
- d) The income generated by its financial resources.

The amounts originating from the collection of the fines indicated in this law will be used to update Prodhab equipment and programs.

The Agency will be subject to compliance with the principles and system of liability established in titles II and X of Law No. 8131, Financial Administration of the Republic and Public Budgets of September 18, 2001. In addition, it must provide the information required by the Ministry of Finance for its studies. Otherwise, the agency is exempt from the scope and application of this law. In its overseeing, the Agency will be subject only to the provisions of the General Controller's Office of the Republic.

SECTION II

INTERNAL STRUCTURE

ARTICLE 21.- Register of files and databases

Any public or private database administered for purposes of distribution, spreading or marketing must be entered in the register to be introduced for this purpose by Prodhab. The registration does not imply the assignment or transfer of the data.

It will be necessary to record any other information imposed by rules with legal rank and the action protocols referred to in article 12 and paragraph c) article 16 of this law.

ARTICLE 22.- Disclosure

Prodhab will prepare and implement a communication strategy intended to allow the citizens to know the rights arising from the handling of their personal data as well as the mechanisms provided by laws for the defense of such rights. It must coordinate with local governments and the Defensoría de los Habitantes de la República [Ombudsman] the periodic disclosure activities among the inhabitants of the cantons.

Furthermore, it will promote among the persons and companies that collect, store or handle personal data the adoption of practices and action protocols suitable to protect their information.

CHAPTER V

PROCEDURES

SECTION I

COMMON PROVISIONS

ARTICLE 23.- Alternative application

In the aspects not expressly set forth in this law, to the extent that they are compatible with its purposes, the provisions of book II of the General Law of Public Administration will be alternatively applicable.

SECTION II

INTERVENTION IN FILES AND DATABASES

ARTICLE 24.- Complaint

Any person who has a subjective right or a legitimate interest may complain to Prodhhab that the public or private database acts in violation of the basic rules or principles for data protection and the self-determination information established in this law.

ARTICLE 25.- Processing of complaints

After receiving the complaint, the controller of the database will be given a term of three business days to give his opinion about the truthfulness of the charges. The person denounced must deliver the evidence backing up his affirmations together with a report, which will be deemed to be given under oath. The omission to issue the report within the stipulated term will cause the charges to be deemed true.

At any time, Prodhhab may order the person denounced to submit the necessary information. Furthermore, it may conduct in situ inspections of its files or databases. To protect the rights of the data subject, it may apply, by motivated act, provisional measures to ensure the effective result of the procedure.

At the latest, one month after the filing of the complaint, Prodhhab must issue the final act. Its decision is subject to appeal for reconsideration filed within three days, which must be resolved in a term of eight days after being received.

ARTICLE 26.- Effects of the resolution in favor of the complainant

If it is determined that the information of the data subject is false, incomplete, inexact, or that according to the rules on personal data protection it was improperly collected, stored or disclosed, it will be necessary to order their immediate elimination, rectification, addition or clarification, or the prohibition of their transfer or disclosure. If the person charged does not fully comply with the order, he will be subject to the sanctions provided in this and other laws.

ARTICLE 27.- Sanctioning procedure

Ex officio, or upon request, Prodhhab may start a procedure to demonstrate whether a database governed by this law is being used according to its principles; for this purpose, it will be necessary to take the steps provided in the General Law of Public Administration for ordinary procedure. The final act will be subject to appeal for reconsideration within three days, which must be resolved within eight days after being received.

ARTICLE 28.- Sanctions

If any of the offenses described in this law were committed, one of the following sanctions must be applied, without prejudice to the corresponding criminal sanctions:

- a) For mild offenses, a fine of up to five base salaries of the position of judicial assistant I, according to the Budget Law of the Republic.
- b) For serious offenses, a fine of five to twenty base salaries of the position of judicial assistant I, according to the Budget Law of the Republic.
- c) For extremely serious offenses, a fine from fifteen to thirty base salaries of the position of judicial assistant I, according to the Budget Law of the Republic, and the suspension of the operation of the file of one to six months.

ARTICLE 29.- Mild offenses

For the purposes of this law, the following will be deemed mild offenses:

- a) Collecting personal data to be used in a database without giving sufficient and ample information to the data subject, pursuant to the specifications of article 5, section I.
- b) Collecting, storing and transmitting personal data of third parties through unsecured mechanisms or mechanisms that do not guarantee in any manner the security and inalterability of the data.

ARTICLE 30.- Serious offenses

For the purposes of this law, the following will be deemed serious offenses:

- a) Collecting, storing, transmitting or otherwise using personal data without the informed express consent of the data subject, pursuant to the provisions of this law.
- b) Transferring personal data to other persons or companies in violation of the rules set forth in chapter III of this law.
- c) Collecting, storing, transmitting or otherwise using personal data for a purpose other than authorized by the data subject.
- d) Denying without justification access to a data subject on the data found in files and databases in order to check their quality, collection, storage and use, pursuant to this law.
- e) Denying without justification to eliminate or rectify the data of a person who requested it by clear and unequivocal means.

ARTICLE 31.- Extremely serious offenses

For the purposes of this law, the following will be deemed extremely serious offenses:

- a) Collecting, storing, transmitting or otherwise using, by private, physical or legal persons, sensitive data according to the definition provided in article 3 of this law.
- b) Obtaining from data subjects or third parties personal data of a person by fraud, violence or threat.
- c) Revealing information recorded in a personal database whose secrecy must be kept according to the law.
- d) Providing to a third party false or different information contained in a data file knowingly.
- e) Processing personal data without being duly recorded with Prodhab in the case of the controllers of databases covered by article 21 of this law.
- f) Transferring to databases in third party countries personal information of Costa Ricans or that of foreigners living in the country without the consent of the data subjects.

SECTION IV

INTERNAL PROCEDURES

ARTICLE 32.- Sanctioning system for public databases

When the controller of a public database commits any of the above offenses, Prodhab will render a resolution establishing the measures to be adopted to stop or correct the effects of the offense. This resolution will be communicated to the controller of the database, to the entity on which he depends hierarchically and the persons affected, if any. The resolution may be rendered ex officio or upon request. The above is without prejudice to the criminal liability incurred.

CHAPTER IV

ROYALTIES

ARTICLE 33.- Royalty for regulation and management of databases

The controllers of the databases that must be recorded with Prodhab, pursuant to article 21 of this law, will be subject to a

royalty for regulation and administration of databases which must be paid annually in the amount of two hundred dollars (\$200), U.S. legal tender. The procedure to collect this royalty will be detailed in the regulation to be issued by Prodhhab for this purpose.

ARTICLE 34.- Royalty for marketing of queries

The controller of the database must pay to Prodhhab a royalty for each sale of data from the files defined in paragraph b) article 3 of this law, of persons that can be identified, legitimately registered and provided it is marketed for profit, ranging between twenty five cents of a dollar (\$0.25) and one dollar (\$1), U.S. legal tender, which amount may be established within said range by regulation. In case of global contracts for low, medium and high consumption of queries, or contractual modalities for online service by number of applications, the regulation of the law will establish the details of the collection of the royalty which may not exceed ten percent (10%) of the contractual price.

TRANSITORY PROVISIONS

TRANSITORY PROVISION I.-

Physical or legal, public or private persons who are currently owners or administrators of the databases covered by this law must adapt their procedures and rules of action as well as the content of their databases to the provisions of this law within a maximum term of one year from the creation of Prodhhab.

TRANSITORY PROVISION II.-

As of the effective date of this law, the process of confirmation and creation of Prodhab will start; for this purpose a maximum term of six months is provided.

TRANSITORY PROVISION III.-

The Executive Power will issue the regulation of this law within a maximum term of six months after the creation of Prodhab, receiving the technical recommendations provided by the Agency.

Valid as of its publication.

GIVEN IN ROOM VII, HEADQUARTERS OF THE SPECIAL PERMANENT DRAFTING COMMISSION.- San Jose the twenty-first day of March, two thousand eleven.

Annie Alicia Saborío Mora

Martín Alcides Monestel Contreras

Alicia Fournier Vargas

Elvia Dicciana Villalobos Argüello

María Eugenia Venegas Renauld

DEPUTIES

o

**G:/redacción/textosplenario/16679R-7-FIN
Prepared by: Kattia**