COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

16 November 2020

T-PD(2020)08

CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA

CONVENTION 108

Evaluation of the Republic of Costa Rica for accession to Convention 108+

by

Franck Dumortier

Directorate General of Human Rights and Rule of Law

Table of contents

Introduction

The mandate of the author of this report is to "produce an analysis of the compliance of Costa Rica's data protection system with Convention 108 +[1] on the basis of the updated legislation transmitted by the country's authorities".

The Costa Rican authorities have transmitted to the Council of Europe the English translations of the following updated legislation:

- Law No. 8968 of 07 July 2011, "Protection of the Individual with Regard to the Processing of its Personal Data";

- Executive Decree No. 37554 of 30 October 2012 (as modified by Executive decree No. 40008 and by Executive Decree No. 41582).

However, for what concerns the latest document, the authorities indicated that "I translated it online, sorry if it have any grammatical error" (sic).

The two aforementioned documents were transmitted to the author of this report in order to conduct his analysis. The rest of the information on which this report is based is issued from desk research carried out by the author.

The author realized this analysis on the basis of the Draft Evaluation Questionnaire (T-PD(2018)20rev) circulated on 17 June 2020 by the Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data.

Executive summary

In the Republic of Costa-Rica, the right to informational self-determination is an extension of the Constitutional right to privacy. The content of this jurisprudential construct was concretized with the adoption of Law No. 8968 of 7 July 2011 on the Protection of the Individual with Regard to the Processing of his Personal Data. This legal norm is being implemented, and sometimes completed, by Executive Decree No. 37554 of 30 October 2012 (as modified by Executive decree No. 40008 and by Executive Decree No. 41582).

Scope of application - The legal framework applies to data processing operations subject to the Costa-Rican jurisdiction in the public and private sectors. The protection is conferred to any individual, regardless of his/her nationality, residence or domicile. Under the legal framework, "personal data" is being understood as "any data regarding any natural person, identified or identifiable". However, it is important to highlight that a distinction is made between "personal data of unrestricted access" − understood as "the contents of public databases of open access, as provided by special laws and in conformity with the purpose for which such data were collected" – and "personal data of restricted access", being defined as "data which, although in records of public access, are not of unrestricted access as they are of interest only to the data subject or to the Public Administration". The main difference between both categories is that

[1] Convention 108 +: Convention for the protection of individuals with regard to the processing of personal data as modernised by the Amending Protocol CETS n°223, available at: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1

“personal data of restricted access” is allowed “solely for public purposes or with the express consent of the data subject” whereas express consent is not be necessary when “it is personal data of unrestricted access, obtained from sources of general public access”. Such a distinction does not exist in the modernised Convention 108 and would only be compliant should the rules on the processing of “publicly available personal data” follow the provisions of Convention 108+.

The regime applies to automated processing and non-automated processing of personal data. In case of manual processing, the personal data must be processed in a “file”, being defined as “any organized set of personal data, whatever the form, purpose or modality of its creation, storage, organization and access”.

Domestic use exemption - The legal framework contains a very broad “domestic use exemption” by excluding from its material scope the “internal databases” processed by any natural or legal person exclusively for internal, personal or domestic purposes, provided such databases are not sold or in any other manner marketed. Any database, file, registry or other structured set of personal data of “restricted or unrestricted access”, maintained by natural persons, is considered as a personal or domestic database, as long as the databases data or its content is not commercialized, distributed or disseminated. Any database, file, registry or other structured set of personal data maintained by legal entities, public or private, is considered as an internal database, as long as the databases or their content is not commercialized, distributed or disseminated. Furthermore, the legal regime does not apply to data referring to natural persons in their capacity as professionals, as long as it is done for the profession's own purposes or in compliance with legal provisions. This distinction narrows the scope of application, contrary to Article 3.2 of Convention 108 + which only excludes data processing carried out by an individual in the course of purely personal or household activities.

Proportionality - The word “proportionality” does not appear as such in the Law nor in the Decree. The law does not provide for the principle of proportionality to be applied at all stages of the data processing, neither does the law provide for the principle of proportionality to be applied at only some stages of data processing. No recommendations nor guidelines from the supervisory authority are to be found to promote compliance with the principle of proportionality at all stages of data processing.

Legitimacy - Under Costa Rican law, free, specific, informed, unambiguous and individualized consent is the only legitimate basis for the processing of personal data of restricted access. Express consent is however not necessary in the following cases: a) when a solid order exists, dictated by a competent legal authority; b) It is personal data of unrestricted access, obtained from sources of general public access; and c) the data must be delivered in accordance with a constitutional or legal provision. As regards, transfers of personal data, these always require the informed consent of the data subject, unless otherwise provided by law.
This part of the Law would seem to require adjustments in order to be fully in line with article 5 of Convention 108 + when it comes to the legitimacy of the data processing and with article 14 in respect of transborder data flows.

Purpose limitation - Personal data must be collected for specified, explicit and legitimate purposes and may not be further processed in a way incompatible with such purposes. Further data processing for historical, statistical or scientific purposes are not considered as incompatible provided that appropriate safeguards are established to protect the data subject rights. However, the nature of these safeguards are not being detailed for what concerns the processing of personal data for historical and statistical purposes. As for the safeguard of anonymizing data for scientific purposes, it only applies to sensitive data. Curiously, article 2, r) of Decree No. 37554 contains a definition of « Disassociation procedure » but this concept is not being used in the operative part of the Decree. This being said, as an exemption to the general rule according to which personal data may not be « be kept ten years after the date on which the registered facts occurred, unless otherwise provided through special regulatory provisions », article 6.1 of the Law foresees that « in cases where data must be stored for longer periods, they shall be unrelated to the relevant data subject ». It would seem appropriate to substantiate further the parts of the Law on purpose limitation to be fully in line with article 4.b of Convention 108 +.

Data quality and limited retention - Personal data may only be collected, stored or utilized for automated or manual processing when such data are current, truthful, accurate and adequate, considering the purposes for which they were collected. When necessary, personal data must be kept up to date. The controller must eliminate data no longer relevant or necessary for the purposes for which they were received and filed. Except when they are "unrelated to the relevant data subject", the conservation of personal data that may affect the data subject in any manner must not exceed a period of ten years after the date on which the registered facts occurred. The Law nevertheless foresees 4 exceptions to this rule: a special regulatory provision establishes another term, the agreement of the parties has established a different term, there is a continuous relationship between the parties or there is a public interest to preserve the data. The provisions on data quality and data retention seem to be in line with Convention 108+, some more clarity would be welcome in view of the application of the four exceptions, to assess their compliance with the general rules set out in article 5.e of Convention 108+ on the retention of personal data, which is that data should not be "preserved in a form which permits identification of data subjects for no longer than is necessary for the purposes for which those data are processed", in conjunction with Article 11 of Convention 108 +.

Sensitive data - Article 3, e) of Data Protection law No. 8968 defines "Sensitive data" as follows: "Information regarding the personal jurisdiction of the individual, such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, socio-economic status, biomedical or genetic information, sexual life and preferences, among others". Compared to article 6 of Convention 108+, the following categories are not listed by the Costa Rican data protection framework: trade-union membership; personal data relating to offences, criminal proceedings and convictions, and related security measures; biometric data uniquely identifying a person. Article 9 of Data Protection law No. 8968 provides that no person is obliged to provide sensitive data. However, this prohibition does not apply in the following cases: a) Data processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; b) Processing is carried out in the course of its legitimate activities and with the appropriate guarantees by a foundation, association or any other body with a political, philosophical, religious or trade-union aim, and on condition that the processing relates solely to the members of the body or to persons who have regular contact with the foundation, association or body, in connection with its purposes, and that the data are not disclosed to a third party without the consent of the data subject; c) The processing relates to data which are manifestly made public by the data subject or are necessary for the establishment, exercise or defence of legal claims; d) The processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of health care or medical treatment or the management of health-care services, and where those data are processed by a health care professional, subject to the obligation of professional secrecy, or by another person also subject to an equivalent obligation of secrecy. Limiting the scope of the processing of sensitive data seems to be in line with the reinforced level of protection provided by Convention 108 + for special categories of data (while the list of data to which the provisions apply do not fully match Article 6 of Convention 108 +) but neither the Law nor the Decree seem to require that additional appropriate safeguards are put in place, else than a narrow provision on security.

Transparency - Article 5 of Data Protection law No. 8968 provides that the controller must inform the data subjects regarding a) the existence of a personal database; b) the purposes pursued by collecting such data; c) the recipients of the information, as well as who may consult such information; d) the mandatory or optional nature of their responses to questions that may be posed while collecting such data; e) the manner in which the data requested will be processed; f) the consequences of refusing to provide the data; g) the possibility of exercising their rights; h) the identity and address of the database controller. In comparison with article 8 of Convention 108 +, the following information are not to be provided to the data subject: the legal basis of the intended processing; the categories of personal data processed. Neither Data Protection law No. 8968 nor the Decree No. 37554 contain any exception to the transparency requirements comparable to the one in Article 11.1 of Convention 108+. However, the transparency principle is subject to the general exemptions from the Citizen´s Right to Self-determination of Data set forth in article 8 of the Law when the following objectives are pursued: a) National security; b) Security and the exercise of public authority; c) Prevention, prosecution, investigation, detention and repression of criminal offences or breaches of ethics in professions; d) Operation of databases used for historical, statistical or scientific purposes, provided there is no risk of identifying individuals; e) Adequate rendering of public services; f) Effective ordinary activities of the Administration performed by official authorities. It seems from the following that additional attention would be needed to bring the national exceptions from transparency requirements in line with all conditions provided for by article 11 of Convention 108 +.

Security - The controller must implement appropriate technical and organizational measures to guarantee the protection of personal data against alteration, accidental or unlawful destruction, loss, unauthorized processing or access and against all other unlawful actions. Such measures must include, as minimum, the most adequate state of the art physical and logical security mechanisms to protect stored data. The controller must determine the security measures applicable to the personal data processed or stored, considering the following factors: a) The sensitivity of the personal data processed, in cases allowed by law; b) The technological development; c) The possible consequences for the data subjects of a violation of the personal data; d) The number of personal data subjects; e) Previous vulnerabilities that occurred in the processing or storage systems; f) The risk to the quantitative or qualitative value that the personal data may have; and g) Other factors arising from other laws or regulations applicable to the controller. In case of a data breach, the controller must inform the data subject of any irregularity in the processing or storage of his data, such as loss, destruction, misplacement, , resulting from a vulnerability of the security of the system or that he learns of, for which he shall have five working days from the moment the vulnerability incident occurred, so that the affected data subjects can take appropriate measures. The provisions of the Law on data security seem to be in line with Convention 108 +, and whether or not requiring the supervisory authority to also be notified in case of a data breach (see article 7.2 of Convention 108+) could also be considered.

Individual's rights - Article 7 of the Data Protection law No. 8968 enumerates the following rights: right to access and right to rectification, update and erasure. Article 7 of the Executive

Decree No. 37554 provides for a right to revocation of consent. Article 13 and 24 of the Data Protection law No. 8968 provides for the right to remedy and the right to assistance from a supervisory authority. Are not listed neither by the Law nor by the Decree: the right not to be subject to automated individual decisions, the right to object and the right to know the reasoning underlying data processing. At the same time the right to access implies that the data subject is provided with " an explanation of the technical terms used" and that data subjects be "informed of the system, program, method or process used to process his personal data". It would thus seem necessary to bring adjustments to those provisions on data subjects' rights, to ensure greater compliance with the ones of Convention 108+.

Additional obligations – Some accountability measures are foreseen in the Law sporadically. For example, the controller must establish and document procedures for the inclusion, conservation, modification, blocking and erasure of personal data, on site or in the cloud, based on codes of minimum conduct and security measures in the processing of personal data. In addition, the controller must undertake as minimum the following actions, which may be required at any time by the Agency: […]develop a risk analysis, which consists of identifying hazards and estimating the risks that may affect the personal data; establish security measures applicable to the personal data and identify those effectively implemented; calculate the existing residual risk based on the difference between the existing security measures and non-existent ones that may be required for the protection of the personal data; develop a work plan for the implementation of the missing security measures based on the result of the assessment of the residual risk. It should be noted that the supervisory authority has no power to approve the result of risk analyses carried out by controllers. Provisions on data controllers' accountability would need adjustments, not to solely concentrate on assessing security but other potential risks representing a potential harm to the rights and fundamental freedoms of data subjects that would need to be mitigated. Principles such as data protection by default and by design would also need to be introduced as provided for by article 10 of Convention108+.

Registration requirement for some databases - All databases, public or private, processed for purposes of distribution, dissemination or marketing must register with the registry established by the supervisory authority and pay the Agency the sum of two hundred dollars of the United States of America (USD $200.00), at the highest sale exchange rate of reference as determined by the Central Bank of Costa Rica on the date such payment is made. This sum is the annual database regulation and administration fee. Processing personal data without being registered with the PRODHAB is considered as a gross offence under article 31, e) of the Law.

International transfers - Neither the Law, nor the Decree contains a section dedicated to international transfers. However, article 31, f) of the Law considers to be a gross offence "To transfer personal data of Costa Rican citizens or foreigners established therein to third countries without the consent of the data subjects". As international data transfers constitute a crucial part in the framework of Convention 108+ , further means to fully apply the provisions of article 14 would need to be assessed.

Exceptions for national security and defense purposes - The principles, rights and guarantees set forth in the legal regime may be restricted in a fair and reasonable manner in accordance with the principle of administrative transparency when the following objectives are pursued: a) National security, b) Security and the exercise of public authority. It is not clear whether PRODHAB or any other body is competent for independent and effective review and supervision of processing activities carried out for national security and defense purposes.

Indeed, the above-mentioned exceptions apply to the exercise of rights, principles but also "guarantees". The extent of the word "guarantees" has not been interpreted in guidelines or communications issued by the supervisory authority. The Costa Rican authorities have not provided to the Council of Europe any specific legislative texts applying to processing activities carried out for national security and defense purposes. No such legislative text has been identified by the author of this report. Hence, it remains questionable whether exceptions for national security and defense purposes are provided for by law, respect the essence of the fundamental rights and freedoms and constitute a necessary and proportionate measure in a democratic society and whether they are only applicable in light of some provisions of the Law in line with article 11. It also remains to be assessed whether other purposes comparable to the ones in article 11.1 and 11.2 for exceptions are covered in the Costa Rican legislation and whether they comply with article 11 of Convention 108 +.

Exceptions for other major legitimate interests of the State - Principles, rights and guarantees set forth in the legal regime may be restricted in a fair and reasonable manner in accordance with the principle of administrative transparency when the following objectives are pursued: a) Adequate rendering of public services, b) Effective ordinary activities of the Administration performed by official authorities. The author of this report has not identified any guidelines nor communications in which PRODHAB or another institution has interpreted or has carried out an effective and independent review and supervision with regard to these exceptions..

Exceptions for the protection of important economic and financial interests - No such exception have been identified by the author of this report. However, it should be noted that article 9.4 of Data Protection law No. 8968 specifies that: "Credit performance data shall comply with the National Financial System regulations so as to guarantee financial entities an acceptable level of risk, without hindering the full exercise of the right to self-determination of data or exceed the limits herein". Article 3, §3 of executive decree No. 37554 adds that "The databases of financial entities that are subject to control and regulation by the General Superintendence of Financial Entities (SUGEF), will not require registration with the Agency for Data Protection of Inhabitants. Notwithstanding the foregoing, the Agency shall have full jurisdiction to regulate and supervise the protection of the rights and guarantees covered under Law No. 8968 and to exercise all the actions granted for this purpose, on said databases".

Exceptions for the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties - The principles, rights and guarantees set forth in the legal regime may be restricted in a fair and reasonable manner in accordance with the principle of administrative transparency when the following objectives are pursued: prevention, prosecution, investigation, detention and repression of criminal offences or breaches of ethics in professions. The author of this report was able to identify the main legal bas/es for exceptions for the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties. These are, amongst others, article 8 of the General Law of Police of 1994; the Law Against Organized Crime of 2009, Law No. 7425 of 1994 on Search and Seizure of Documents and Intervention on Private Communications and Article 40 of Law No. 5524 establishing the Criminal File. In order to assess the compliance of the national legislation with Convention 108 + all other relevant legislations would need to be analysed as well.

Other Sectoral Data Protection Law and codes of conduct - Article 42 of the General Telecommunications Law No. 86423 guarantees the privacy of communications and protection of personal information. There is a complementary administrative regulation Nº 35205-

MINAET that guarantees the secrecy of communications, the right to privacy, and the protection of personal data of subscribers and users.

Supervision & enforcement – The supervisory authority is the Agencia de Protección de Datos de los Habitantes (Inhabitant Data Protection Agency - PRODHAB). It has its own legal identity to perform the duties assigned and manage its own resources and budget. The Agency may sign contracts and agreements as necessary to perform its duties. The Agency enjoys independence to emit judgement. The author of this report has not identified the existence of an annual activity report. According to PRODHAB's website, in 2019, 96 complaints were handled. PRODHAB's decisions are not being published.

Public awareness raising activities - PRODHAB issues press releases on specific topics to promote public awareness on the rights of data subjects and on the responsibilities of controllers. Furthermore, PRODHAB has active accounts on Facebook and Twitter through which the authority conducts campaigns to promote data protection awareness. The author of this report did not identify any survey results on the level of public awareness.

System to receive complaints from individuals - Regardless of their nationality, residence or address, the system made available to individuals to submit complaints can be found on PRODHAB's website. At any time, PRODHAB may order any person to submit the necessary information and may perform on-site inspections of such databases or files. To protect the data subject's rights, the Agency may order, by justified decision, precautionary measures to ensure the effective outcome of the process.

Sanctions and remedies - The PRODHAB may, on its own account or upon request of a party, initiate a procedure to verify whether a database under this law is being used according to its principles. In order to comply with this, the PRODHAB must follow the steps established in the General Public Administration Law for the ordinary procedure. A request for reconsideration of the final decision may be requested within three days of its issuance, and a reply must be provided within eight days of receiving such request. Monetary sanctions are foreseen in Article 28 of Data Protection law No. 8968.

It follows from the above that provisions on the national supervisory authority seem to be broadly in line with Chapter IV of Convention 108 +, however some additional attention would be needed to check the implementation of provisions regarding the independence, powers and functions of the authority and whether its functioning fulfils requirements set forth in Chapter V of Convention 108+ on cooperation and mutual assistance.

Section I – Political organisation and general institutional context of Costa Rica

1. Political structure

Costa Rica gained independence from Spain on 15 September 1821. An immediate challenge for the country after independence was the need to decide whether to remain independent or join the Mexican Empire. Disagreement led to the Civil War of Costa Rica that ended in 1823 when the pro-independence side won and created the capital, San José. In 1838, the country withdrew from the Federal Republic of Central America and became fully sovereign. Since then, Costa Rica is a free and independent democratic Republic[2]. The area of Costa Rica is 51,100 km² of which 51,060 km² is land and 40 km² is water. The country is bordered by Nicaragua to the north, Panama to the south-east, the Caribbean Sea to the east and the Pacific Ocean to the west. According to population estimates and projections, Costa Rica's population reached 5,000,000 on 1 September 2018. The national language of Costa Rica is Spanish[3]. People living on the country's Caribbean shores speak English, and there are also a number of indigenous ethnic groups that have their own languages.

Sovereignty resides exclusively in the Nation[4]. The State is unitary. The Government of the Republic is popular, representative, participatory, alternate and responsible. It is exercised by three distinct and independent branches: Legislative, Executive, and Judicial[5]. Executive power is exercised, on behalf of the people, by the President of the Republic and ministers as subordinate collaborators[6]. The People delegate, by vote, their power to legislate to the Legislative Assembly, which consists of 57 members[7].

Main control of the country lies in the hands of the central government which is headed by the President. However, administrative divisions in Costa Rica consist of 7 provinces (provincias): San Jose, Heredia, Alajuela, Cartago, Puntarenas, Guanacaste and Limon. All provincial capital cities, with the exception of Guanacaste's Liberia, share the same name as their province. These provinces are then further divided up into 82 cantons (cantones). San Jose is the largest province with 20 cantons, Alajuela with 16, Heredia with 10, Cartago with 8, Guancaste with 11, Puntarenas with 11 and Limon with 6. The cantons in turn are divided into districts (districtos). Cantons are the only administrative division in Costa Rica that possess local governments in the form of municipalities (municipalidad). Each municipality consists of two bodies: a municipal executive (Concejo Municipal) and an executive body which only consists of a mayor (alcalde / alcaldesa municipal).

2. Relation between domestic and International law

According to article 7 of the Constitution, public treaties, international agreements and concordats duly approved by the Legislative Assembly have a higher authority than the laws upon their enactment or from the day that they designate.

Under Article 7 of the Constitution, public treaties and international conventions duly approved by the Legislative Assembly take precedence over the laws. The Constitutional Chamber also recognized, on the basis of Article 48, that the human rights instruments in force in Costa Rica not only have a value similar to that of the Constitution, but also, when they bestow superior rights or guarantees upon people, prevail over the Constitution (Constitutional Chamber Judgement No 3435-92).

With regard to the suspension of internationally recognized commitments, article 121.7 of the Constitution of 11 November 1947 authorizes the Legislative Assembly to suspend the

[2] Article 1 of the Constitución de la República de Costa Rica de 1949. A translation to English of the Constitution is available at https://costaricalaw.com/costa-rica-legal-topics/constitutional-law/costa-rica-constitution-in-english/
[3] Ibid, article 76.
[4] Ibid, article 2.
[5] Ibid, article 9.
[6] Ibid, article 130.
[7] Ibid, articles 105 and 106.

following individual rights and guarantees for reasons of obvious public necessity for a period of up to 30 days: freedom of movement, the inviolability of the home and other premises, the privacy of communications, freedom of peaceful assembly, freedom of opinion, freedom of expression in speech or writing, access to administrative departments and the presumption of innocence.

As a result of the country's political, economic, social and cultural stability, no such suspension has been decreed by the Legislative Assembly, thus ensuring the enjoyment of human rights for the past 70 years.

This being said, in the context of the COVID-19 pandemic, through Executive Decree N°42227-MP-MS published in March 16 of this year, the Executive Power, has declared the state of national emergency in the whole territory of the Republic of Costa Rica, due to the situation of health emergency. By consequence, the data protection authority has temporarily suspended its services for one month as well as the terms in all procedures regulated by Data Protection Law N°8968 and its Regulations[8].

3. Separation of powers

As stated in article 9 of the Constitution, the political structure of the Republic of Costa Rica has three distinct and independent branches: legislative, executive and judicial. None of these Branches may delegate the exercise of their own functions.

- Article 130 provides that executive authority is exercised, in the name of the people, by the President of the Republic and the government ministers, who are required to work together.

- Under articles 105 and 106 of the Constitution, the Legislative Assembly is given the power to make laws and has 57 deputies, who are elected by the people. Deputies are elected every four years in elections with a closed-list system, universal suffrage and secret ballots, and may not stand for immediate re-election. In accordance with article 106 of the Constitution, deputies are elected by the provinces, and the Supreme Electoral Tribunal apportions to each province, in proportion to its population, a number of seats in the Legislative Assembly. In accordance with article 99 of the Constitution, the Tribunal has sole jurisdiction over the organization, conduct and supervision of proceedings relating to suffrage and has the independence necessary to carry out its mandate. Other electoral bodies are responsible before the Tribunal.

- Article 9 of the Constitution establishes the judiciary, a branch of state administration independent of the Executive and the Legislative Assembly, to administer justice in Costa Rica. The judicial power is exercised by the Supreme Court of Justice and by other courts established by law[9]. Article 10 foresees that a specialised Chamber of the Supreme Court of Justice may declare, by an absolute majority vote of its members, the unconstitutionality of provisions of any nature and of acts subject to Public Law. This Chamber may also settle any conflicts of jurisdiction between State branches, including the Supreme Electoral Tribunal, as well as any other entities or bodies established by

[8] PRODHAB, Resolución N° 07-001-2020, 13 de julio de 2020, available at http://prodhab.go.cr/download/COMUNICADOS/Resolucionsuspensiondeplazos.pdf
[9] Ibid, article 152.

> law. In addition, the Judicial Branch is entrusted to hear civil, criminal, commercial, labour, and administrative-litigation cases, as well as any others established by law, regardless of their nature or the status of the persons involved and execute the decisions that they deliver , if necessary, with the help of the police.[10].

The Supreme Court of Justice is the highest court of the Judicial Branch. For the administration of justice, the Supreme Court is divided into four chambers: three Chambers of Cassation and the Constitutional Chamber. The overall function of the three Chambers of Cassation is to hear appeals on points of law, each in its area of specialization; that is, their role is to review the rulings of collegiate courts to ensure that they are lawful on procedural grounds and in terms of the merits, thereby harmonizing standards and setting precedents. The First Chamber, for example, hears appeals on points of law and applications for judicial review of the facts of the case in ordinary or summary proceedings relating to civil, commercial and administrative disputes. It also functions as a court of third instance for agricultural matters and gives effect to judgments handed down abroad. The Second Chamber is responsible for appeals on points of law and applications for judicial review of the facts of the case in ordinary or summary proceedings relating to family and inheritance matters. It also acts as a court of third instance for labour matters. The Third Chamber hears appeals on points of law and applications for judicial review of the facts of the case in criminal matters and in proceedings against government officials. The Supreme Court's Fourth Chamber is the Constitutional Chamber. The Constitutional Chamber is governed not only by the Constitution but also by Act No. 7135 of 11 October 1989. Its role is to guarantee the supremacy of constitutional rules and principles and of the international or community law in force in Costa Rica, the uniform interpretation and application of those rules, principles and laws, and the fundamental rights and freedoms enshrined in the Constitution or international human rights instruments applicable in the country. Between 2000 and 2017, the Constitutional Chamber handled a total of 292,304 applications, including applications for amparo, writs of habeas corpus and unconstitutionality actions[11].

Persons residing in Costa Rican territory may submit applications for writs of habeas corpus or a remedy of amparo. In accordance with article 48 of the Constitution and articles 15 to 28 of Act No. 7135 of 11 October 1989, the Constitutional Jurisdiction Act, habeas corpus is used to guarantee a person's right to freedom and safety when that right is violated or threatened by illegitimate restrictions, acts or omissions on the part of the authorities or by unlawful detention. Its scope includes freedom, bodily integrity, freedom of movement, the right of residence in the country and the right of entry and exit. Anyone may file an application for a writ of habeas corpus; no legal adviser or lawyer is needed. The applicant may file the application on his or her own behalf or on behalf of another person. In vote No. 0878-97, the Constitutional Chamber stated that the remedy of habeas corpus is not a measure designed solely to order the restoration of the applicant's freedom but a genuine constitutional process whose purpose is not only to safeguard the rights of personal freedom and integrity in the future but also to establish violations in the past and to require the authority responsible for any such violation to compensate the victim for damages and pay the applicant's costs. Within the framework of the Constitution and the Constitutional Jurisdiction Act, the remedy of habeas corpus is (a) a means of redress: this type of remedy is used to provide redress to or restore the freedom of persons who have been illegitimately deprived thereof because of a failure to proceed in accordance with domestic legislation; (b) preventive: here its purpose is to prevent threats of deprivation of

[10] Ibid, article 153.

[11] See UN, Office of the High Commissionner for Human Rights, Common core document forming part of the reports of States parties, Costa Rica, 26 March 2019, HRI/CORE/CRI/2019, p.

liberty, including arbitrary threats; (c) corrective: here its purpose is usually to change a prisoner's place of detention, either because it is not suited to the nature of the crime or because the prisoner is being subjected to improper treatment; and (d) injunctive: here its purpose is to put an end to the unwarranted persecution of an individual by the judicial or administrative authorities or to the obstruction of his or her access to public or private premises. Seen in this way, the broad scope of the legislation enables the Constitutional Chamber to exercise full oversight over any act or omission that, currently or in the future, may restrict or threaten to restrict any of the rights protected by the Constitution.

Under article 48 of the Constitution and articles 29 to 72 of the Constitutional Jurisdiction Act, amparo proceedings may be brought against a private or public party with a view to maintaining or restoring enjoyment of other rights enshrined in the Constitution and the fundamental rights established in international human rights instruments in force in Costa Rica. The scope of this remedy therefore includes rights such as the right to life, honour, equality, the freedoms of opinion, thought, information, worship and association, and rights related to the family, childhood and the environment. Amparo may be invoked against any provision or decision and, in general, against any action, omission or simple physical act not based on a valid administrative disposition, committed by public servants or public bodies, and that has violated, violates or threatens to violate any of those rights, as well as against arbitrary actions and acts or omissions based on misinterpreted or improperly applied regulations. Amparo is also used to safeguard the human rights recognized in international law in force in Costa Rica. This is an important innovation, for there are fundamental rights enshrined in international treaties which are not expressly recognized in the Costa Rican Constitution, such as the right of correction or reply. Under article 57 of the Constitutional Jurisdiction Act, an action for amparo may also be brought against "acts or omissions by subjects of private law when they are acting or should be acting in the exercise of public functions or powers or when they find themselves de jure or de facto in a position of power against which the ordinary legal remedies are clearly insufficient or too slow to guarantee the fundamental rights and freedoms referred to in article 2 (a) of the Act".

4. Independence of the judiciary

The independence of the judiciary from other branches of government is enshrined in articles 9, 153 and 154 of the Constitution.

According to article 154 of the Constitution, the Judicial Branch is subject only to the Constitution and the law, and its decisions on matters within its jurisdiction impose no responsibilities other than those specifically set forth in legislation.

All courts, officials and employees of the Judicial Branch are subordinate to the Supreme Court of Justice, without prejudice to any provisions contained in the Constitution concerning civil service[12]. The Supreme Court has justices who are elected by the Legislative Assembly for a term of eight years[13].

[12] Ibid, article 156.
[13] Ibid, article 158.

Section II – Data Protection Laws

1. International commitments

The status of Costa Rica in main human rights instruments is indicated below:

Instrument	*Ratification*
International Covenant on Economic, Social and Cultural Rights (1966)	29 November 1968
International Covenant on Civil and Political Rights (1966)	29 November 1968
Optional Protocol to the International Covenant on Civil and Political Rights, concerning communications from individuals (1966)	29 June 1968
Second Optional Protocol to the International Covenant on Civil and Political Rights, aiming at the abolition of the death penalty (1989)	5 June 1998
International Convention on the Elimination of All Forms of Racial Discrimination (1965)	4 April 1986
Convention on the Elimination of All Forms of Discrimination against Women (1979)	4 April 1986
Optional Protocol to the Convention on the Elimination of All Forms of Discrimination against Women, concerning complaints from individuals and inquiry procedures (1999)	20 September 2001
Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (1984)	11 November 1993
Optional Protocol to the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, concerning regular visits by national and international institutions to places of detention (2002)	1 December 2005
Convention on the Rights of the Child (1989)	21 August 1990
Optional Protocol to the Convention on the Rights of the Child on the involvement of children in armed conflict (2000)	24 January 2003
Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography (2000)	9 April 2002
International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families (1990)	Not ratified

At regional level, Costa Rica is a member of the regional human rights mechanism provided for by the American Convention on Human Rights (ACHR) – also known as the “Pact of San Jose”– adopted by Act No. 4534 of 23 February 1970 and ratified on 8 April 1970. Within the framework of this mechanism, the competence of the Inter-American Commission on Human

Rights and the Inter-American Court of Human Rights with respect to matters relating to the fulfilment of the provisions of the Convention, was accepted[14].

As a reminder, Article 11 of the ACHR warrants the right to privacy as follows:

> *"1. Everyone has the right to have his honor respected and his dignity recognized.*
> *2. No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation.*
> *3. Everyone has the right to the protection of the law against such interference or attacks".*

In case of Artavia Murillo et al. (In Vitro Fertilization) v. Costa Rica[15], the Court held that:

> *"Every person has the right to organize, in keeping with the law, [his] individual and social life according to [his] own choices and beliefs […]. The Court has also underscored the concept of liberty and the possibility of all human beings to self-determination and to choose freely the options and circumstances that give meaning to their life, according to their own choices and beliefs"[16].*

The scope of the protection of the right to private life has been interpreted in broad terms by the international human rights courts, when indicating that this goes beyond the right to privacy. The protection of private life encompasses a series of factors associated with the dignity of the individual, including, for example, the ability to develop his or her own personality and aspirations, to determine his or her own identity and to define his or her own personal relationships. The concept of private life encompasses aspects of physical and social identity, including the right to personal autonomy, personal development and the right to establish and develop relationships with other human beings and with the outside world. The effective exercise of the right to private life is decisive for the possibility of exercising personal autonomy on the future course of relevant events for a person's quality of life. Private life includes the way in which individual views him/herself and how he/she decides to project this view towards others, and is an essential condition for the free development of the personality. Furthermore, the Court has indicated that motherhood is an essential part of the free development of a woman's personality[17].

---

[14] Costa Rica declared that it recognizes, without conditions and while the American Convention on Human Rights remains in effect, the competence of the Inter-American Commission to receive and examine communications in which a State Party alleges that another State Party has committed a violation of human rights established by the cited Convention. Costa Rica also declared that it recognizes, without conditions and while the American Convention on Human Rights remains in effect, the mandatory jurisdiction of the Court, as a matter of law and without a specific convention on the Inter-American Court on Human Rights, on all cases relating to the interpretation or application of such multilateral treaty. See http://www.oas.org/dil/treaties_b-32_american_convention_on_human_rights_sign.htm

[15] Artavia Murillo et al. (In Vitro Fertilization) v. Costa Rica , November 28, 2012. Series C No. 257.

[16] Ibid., § 142.

[17] Ibid., §143.

2. Constitutional protection

The Constitution of the Republic of Costa Rica was enacted by the Members of the National Constitutional Assembly after the revolution of 1948. It was adopted on 7 November 1949[18].

2.1. Protection of the domicile and private premises

Article 23 of the Constitution, establishes that:

> *"The domicile and all other private premises of the inhabitants of Costa Rica shall be inviolable. However, they may be searched under written warrant from a competent judge, either to prevent an offence being committed or going unpunished or to prevent serious harm to persons or property, as provided by law".*

Constitutional Chamber case law holds that "article 23 of the Constitution establishes that the private premises of citizens are inviolable except in cases expressly authorized by law and under a written warrant issued by a competent court. Entry to a person's home must only be effected in exceptional cases, with the intervention of the administrative police as requested by the court, and in the presence of the judge. When the judge cannot attend or take part in a house search the task can be delegated to the judicial police, but only in cases where there is proper justification for such absence, since the court is responsible for the conduct of such operations".[19]

In terms of specific cases, the Constitutional Chamber has handed down many rulings on the application of this article. One example is decision No. 13417-05, in which the Chamber upheld an appeal against inclusion in a criminal record of a sentence the person had served over 10 years previously, and which had apparently not been expunged because the full sentence had not been served. The judgement ordered the Head of the Archive and Judicial Register "to take immediate steps to remove the entry containing the judgement against the applicant, handed down by the third Higher Criminal Court of San José, Section II, in respect of which the sentence was declared extinguished by ruling of the visiting magistrate of the first San José district circuit court at 10.40 a.m. on 21 June 2004".

2.2. Right to intimacy, freedom and secret of communications

The Constitution does not protect "privacy" as such, but its Article 24 reads:

> *"The right to intimacy, freedom and secret of communications is guaranteed".*

Furthermore, Article 24 was amended by Article 1° of Law N° 7607 of 29 May 1996[20] by adding the following:

> *"Private documents and written, verbal or other communications of the inhabitants of the Republic are inviolable. However, a law, which enactment and amendment shall require the vote of at least two thirds of the entire membership of the Legislative Assembly, shall determine those cases in which Courts of Justice may order the seizure,*

[18] Constitución de la República de Costa Rica de 1949. A translation to English of the Constitution is available at https://costaricalaw.com/costa-rica-legal-topics/constitutional-law/costa-rica-constitution-in-english/

[19] See Constitutional Chamber decisions No. 2929-96 and No. 5903-94.

[20] Ley nº 7607 de 29 de mayo de 1996. Reforma de los artículos 24 y 46 de la Constitución de Costa Rica.

search, or examination of private documents, whenever this is absolutely necessary to clarify matters submitted to their cognizance.

Likewise, this law shall determine the cases in which Courts of Justice can order the intervention of any communication and indicate the offenses in which investigation the exercise of this exceptional investigatory power can be authorized, and the period of time during which such an intervention shall be permitted. The law shall also determine the responsibilities and penalties of any officials who apply illegally this exception. Any judicial resolution under this provision shall be duly reasoned and can be immediately enforced. Its application and control shall be the responsibility of judicial authorities and cannot be delegated.

The law shall also determine in what instances competent officials of the Ministry of Finance and the Office of the Comptroller General of the Republic may examine accounting books and related documents for fiscal purposes as well as to control the correct use of public funds.

A special law, passed by two thirds of the entire membership of the Legislative Assembly, shall determine which other bodies of the Public Administration shall be authorized to examine the documents established by said law in the performance of their duties of regulation and control for public ends. This law shall also provide the cases when such an examination is appropriate.

Any correspondence seized or information obtained as a result of the illegal intervention of any communication shall have no legal effect".

2.3. Right to data protection

The Constitution does not protect the "right to data protection" as such.

However, the Constitutional Chamber has recognized the existence and the validity of a right for individuals to control and protect their personal data as follows:

« The Right to Privacy implies the recognition and acceptance of the fundamental right of every individual or legal entity to know what is recorded about them, their assets or rights in any record or file, of any nature, including mechanical, electronic or computerized, whether public or private; as well as the purpose for which such information is intended and, if applicable, to have it rectified, updated, supplemented or deleted, when the subject considers that it is incorrect, inaccurate or that it implies discrimination. The same as not to be used or disclosed improperly and respect its legitimate confidentiality. The purpose of this right is that any person has the possibility to defend himself against suspicious qualifications included in records that, without giving him the right to rectify or contradict them, could cause him serious harm »[21].

Nonetheless, the need for a law that would positivize the principles derived from the jurisprudence was emphasized, as well as the need to reinforce the protection of the inhabitants of the country against any undue violation of this right. An expectation that became a reality in 2011 with the enactment of the Law for the Protection of the Person against the Processing of

[21] Constitutional Chamber, vote No. 1345-1998 at 11:36 a.m. on February 27, 1998

Personal Data[22]. It should be noted that although constitutional jurisprudence, *ab origine*, pointed out that the right to privacy was a basis for recognizing the fundamental right to the protection of informational self-determination, it soon warned that its protection went beyond the simple scope of privacy. In this regard, it is worth quoting Ruling No. 11257-2006 of 9:23 a.m. on 1 August 2006, which states:

> *« In summary, then, it follows that informational self-determination is an extension of the right to privacy and that its protection arises from the development of global computer and technological mechanisms that manage databases containing information on individuals. "In fact, it is clear that the Law on Protection of Individuals with regard to the Processing of their Personal Data establishes a regime for the protection of personal data and its essential objective is to guarantee any person their right to informational self-determination ».*

In the same vein, the Constitutional Chamber (No. 5268-2011 of 27 April 2011*)* held that:

> *« It is important to point out that the law fills an important normative void related to the right to informative self-determination, that although the jurisprudence of the Chamber has taken care of developing its content, there persists the need to develop an administrative institution that watches over a balance in the activity, and so that it constitutes a first line of specialized defense of this fundamental right ».*

Accordingly, article 4 of the Law No. 8968 provides that:

> *"Every individual has the right to self-determination of data, including principles and guarantees regarding the lawful processing of the personal data under this section.*
> *Self-determination of data is also recognised as a fundamental right, aimed at controlling the flow of information regarding each individual, which results from the right to privacy, and at discouraging discriminatory actions".*

Article 12 of Executive decree No. 37554 of 30 October 2012 defines the right to self-determination of data as follows:

> *"It is the fundamental right of any natural person to know what is contained about him, his assets or rights in any database, of any type, public or private, the purpose for which his personal information is being used or collected, as well as to demand it be rectified, updated, supplemented or erased in the event it is incorrect or inexact, or if it is being used for a purpose other than the one authorized or others that it can legitimately fulfil".*

3. Data protection norms

3.1. Data Protection law No. 8968

Law No. 8968 of 07/07/2011 is entitled "Protection of the Individual with Regard to the Processing of its Personal Data". This law is structured in six chapters:

[22] Law No. 8968 of 07/07/2011, "Protection of the Individual with Regard to the Processing of its Personal Data", La Gaceta No.: 170 of 05/09/2011.

- Chapter I provides for general provisions: objectives and scope[23], scope of application[24], definitions[25];

- Chapter II lays down the basic rights and principles for personal data protection. This chapter is divided as follows:

  - Section 1 lists the basic rights and principles: right to self-determination of data[26], principle of informed consent[27], principle of data quality[28], rights of the individual[29], exemptions to the citizen´s right to self-determination of data[30];

  - Section 2 provides for additional rules applying to special data processing categories[31];

  - Section 3 contains provisions applying to data processing security and confidentiality: duty of data security[32], duty of confidentiality[33], codes of conduct[34], effective guarantees for data subjects[35].

- Chapter III consists of one general rule applying to personal data transfers[36];

- Chapter IV relates to the data protection authority and is divided as follows:

  - Section 1 establishes the Inhabitant Data Protection Agency (PRODHAB)[37], lists its powers[38], regulates the agency management[39] and staff[40], the prohibitions applying to PRODHAB employees[41] and the agency's budget[42];

  - Section 2 imposes the registration of files and databases to the agency[43] and foresees the agency's communication/dissemination strategy to inform data subjects about their rights[44];

- Chapter V is composed of 3 sections:

[23] Article 1 of Law No. 8968
[24] Article 2 of Law No. 8968
[25] Article 3 of Law No. 8968
[26] Article 4 of Law No. 8968
[27] Article 5 of Law No. 8968
[28] Article 6 of Law No. 8968
[29] Article 7 of Law No. 8968
[30] Article 8 of Law No. 8968
[31] Article 9 of Law No. 8968
[32] Article 10 of Law No. 8968
[33] Article 11 of Law No. 8968
[34] Article 12 of Law No. 8968
[35] Article 13 of Law No. 8968
[36] Article 14 of Law No. 8968
[37] Article 15 of Law No. 8968
[38] Article 16 of Law No. 8968
[39] Article 17 of Law No. 8968
[40] Article 18 of Law No. 8968
[41] Article 19 of Law No. 8968
[42] Article 20 of Law No. 8968
[43] Article 21 of Law No. 8968
[44] Article 22 of Law No. 8968

- Section 1 foresees the supplementary application (combined legal application) of the provisions of Book II of the General Law of Public Administration if compatible with the purposes of this Law[45];

- Section 2 regulates the means of redress of the data subjects towards private and public databases. For what concerns private databases, this section states that any person with a subjective right or legitimate interest may lodge a claim with the PRODHAB[46], details the procedure to be followed[47], the effects of the agency's decision[48], the procedure relating to administrative sanctions[49] as well as, without detriment to other applicable criminal sanctions, the types of sanctions[50] for minor[51], serious[52] and gross[53] offences;

- Section 3 foresees the sanctions the PRODHAB can pronounce regarding public databases;

• Chapter VI enacts the fees that database controllers must pay to the PRODHAB;

• Finally, the law foresees temporary provisions. The most crucial one (Temporary provision III) provides that the executive branch shall issue the regulations applicable to this law, addressing the technical recommendations provided by the PRODHAB[54]. In view of the foregoing, by Executive Agreement N° 212-MJP dated 22 November 2011, published in the Official Journal La Gaceta N° 11 of 16 January 2012, the Executive Power formed an Inter-Institutional Commission and assigned it the responsibility of drafting the Regulations to the above-mentioned Law.

3.2. Executive decree No. 37554

Executive Decree No. 37554 of 30 October 2012[55] (as modified by Executive decree No. 40008[56] and by Executive Decree No. 41582[57]) is entitled "Regulations to the Law on the Protection of the Individual with Regard to the Processing of its Personal Data". This decree was adopted according to the mandate given to the executive branch to issue the regulations implementing Law No. 8968.

The decree is composed of 10 chapters as follows:

- Chapter I provides for general provisions: object; definitions, initials and acronyms; scope of application;

[45] Article 23 of Law No. 8968
[46] Article 24 of Law No. 8968
[47] Article 25 of Law No. 8968
[48] Article 26 of Law No. 8968
[49] Article 27 of Law No. 8968
[50] Article 28 of Law No. 8968
[51] Article 29 of Law No. 8968
[52] Article 30 of Law No. 8968
[53] Article 31 of Law No. 8968
[54] Temporary provision III of Law No. 8968
[55] Executive Decree n°37554 of 30/10/2012 "Regulations to the Law on the Protection of the Individual with Regard to the Processing of its Personal Data".
[56] Executive Decree No. 40008 of 19 July 2016.
[57] Executive Decree No. 41582 of 21 Februari 2019.

- Chapter II details the requirements for consent, the formalities of consent, the burden of proof for consent, revocation (and process of revocation) of consent, term of the controller to confirm the revocation, claims a data subject may file in case of rejection of revocation. Finally, this section explicitly states that *“ the conservation of personal data that may affect the data subject shall not exceed a term of ten years from the date the recorded facts occurred, except in the event a special provision exists that establishes another term or because the agreement between the parties established a shorter term. In case conservation beyond the established term is necessary, the personal data must be disassociated from the data subject”*;

- Chapter III defines the Right to Self-Determination of Data (this concept covers the rights to information, access, rectification, update, modification and erasure), the modalities of exercise of the rights, restrictions to the exercise of the rights, the persons empowered to exercise the rights, the means and forms to exercise the rights as well as their requirements, the delay in which the controller must process the data subjects' requests, requirements for the controller to ask additional information to process the data subjects' requests, the responses a controller must provide to requests. This Chapter also details the right to access and its means, the right to rectification and its requirements, the right to elimination or erasure;

- Chapter IV imposes the controller duties of documentation (accountability), liability, conditions for subcontracting, obligations of the processor, the content of codes of minimum conduct a controller must impose to processors and the powers of the PRODHAB to verify the compliance to these codes. This chapter also details the controller's duty of security, the factors to determine applicable security measures, a method for risk analysis and requirements to update security measures. Finally, this chapter imposes data breach communication and the minimum information to be disclosed in such cases;

- Chapter V contains the conditions for transfer which includes the marketing of personal data, it also imposes compliance with codes of minimum conduct in case of such transfers, foresees the burden of proof for compliance in case of such transfers, and, finally imposes contracts in case of such transfers.

- Chapter VI details the duty to registrate databases and filing systems with the PRODHAB (as well as the procedure of verification/rectification of the registration, fees, inadmissibility decision, cancellation of database registration records, and challenge procedure). Finally, this chapter foresees the powers of the agency to verify possible breaches to databases and filling systems.

- Chapter VII relates to the claims which may be lodged with the agency to protect data subjects' rights, their grounds, requirements, documentary evidence and admissibility. It also provides that the agency may order precautionary measures, the procedure to be followed for such decisions, the transfer of charges, forms of evidence, sanctions and means of challenge.

- Chapter VIII details the administrative collection procedure to be followed when monetary sanctions or fees are not paid, fines and arrears interest in case of late payment, plea bargaining criterion and procedure for legal collection as well as requirements for out-of-court payments.

- Chapter IX details the annual database regulation and administration fee to be paid to the PRODHAB; the term to pay; the fee to be paid for the sale of filing system data; fees that apply to controllers with global contracts for low, medium or high consultation volumes, or on-line service contracts by number of application; fines and arrears interest and collection procedure in case of non-compliance.

- Chapter X relates to the employment regime of the PRODHAB, the selection procedures for staff and the trial period.

4. Scope of application

4.1. Territorial scope

The territorial scope of the general Costa Rican data protection law is not defined in Data Protection law No. 8968 but in the executive decree No. 37554, of which article 3 states:

> *"This Regulation will be applied to the personal data that appear in the automated or manual databases of public or private organizations, and to any form of subsequent use of these data, as long as they take effect within the national territory, or the Costa Rican legislation derived from the conclusion of a contract or under the terms of international law."*

Besides this provision, some elements regarding the territorial scope can be found in article 1 of said decree:

> *"The purpose of these provisions is to regulate the Law on the Protection of the Person from the Treatment of their Personal Data, in terms of guaranteeing to any individual, regardless of their nationality, residence or domicile, respect for their fundamental rights, specifically, their right to informative self-determination in relation to your privacy or private activity, as well as the defense of your freedom and equality with respect to the automated or manual treatment of the data corresponding to your person or property".*

4.2. Notion of personal data

Article 3, b) of Data Protection law No. 8968 defines personal data as being *"any data regarding any natural person, identified or identifiable"*.

Furthermore, article 2, q) of the executive decree No. 37554 defines an identifiable natural person as a *"person whose identity can be determined, directly or indirectly, by means of any information referring to their anatomical, physiological, psychological, economic, cultural or social identity. A natural person will not be considered identifiable if such identification requires time limits or disproportionate activities".*

The Constitutional Chamber (vote No. 2017-004786 of March 29, 2017) has ruled that an employer may request the password of the official mail of an institution. It does not include a worker's institutional mail (which may imply identification with name or surname). PRODHAB communicated that the password of the institutional mail of each collaborator, even though supported by the electronic property of the employer, must remain private and confidential[58]. According to PRODHAB:

> *"Although, by vote No. 2017-004786 of March 29, 2017, the Chamber declared that it is correct that an employer requests the password of the official mail of an institution, this is a sign that does not include a worker's institutional mail. Accordingly, mail that a company or institution assigns independently to each of its collaborators, and which even implies an identification such as their name or surname, is keeps it unscathed. Not so the official mail of an institution, which is not a private account since channels information related to the interests of the organization as such and not of a individual. This is where official communications are handled or aired, which are spring direct from the entity to which it belongs. As for the institutional mail of each collaborator, although it is in a support electronic property of the employer, your password must remain private and unique knowledge of each holder. It is worth mentioning that the use of this last mail must be governed according to the policies that have agreed between the employee and his/her employer, in order to safeguard the responsibilities of each. The Agency considers it appropriate to make the clarification, in the interest of making the observation in a to those companies or institutions that, by mistake, have misinterpreted this vote of the Chamber and thus prevent them from incurring in possible breaches of the personal data in force".*

Interestingly, article 3, g) of Law No. 8968 defines "data subject" as *"an individual, <u>owner of the data</u> that are object of automated or manual processing"*. Article 2, v) of the executive decree No. 37554 defines "owner or interested party" as the *"natural person owning the personal data protected by Law, or his representative"*.

It is also important to note that the Data Protection law No. 8968 differentiates between several categories of personal data:

- Personal data of unrestricted access: *"the contents of public databases of open access, as provided by special laws and in conformity with the purpose for which such data were collected"*[59]. Article 9.3. of Data Protection law No. 8968 provides that *"personal data of unrestricted access are contained in public databases of open access, as provided by special laws and according to the purposes for which they were collected. This category does not include: exact home address, unless required for a mandate, citation or administrative or judicial notification, or for a financial or bank operation, photograph, private telephone numbers and similar, the processing of which may affect the rights and interests of the data subject"*. Furthermore, Article 2, d) of executive decree No. 37554 defines *"public access databases" as being "those files, files, registry or other set of data structures that can be consulted by anyone who is not impeded by a limiting rule, or with no other requirement than the payment of a consideration"*.

- Personal data of restricted access: *"data which, although in records of public access, are not of unrestricted access as they are of interest only to the data subject or to the*

[58] See PRODHAB, « La clave del correo institucional continúa siendo privada », Comunicado de prensa 05 de mayo, 2017, available at http://prodhab.go.cr/download/COMUNICADOS/laclavedelcorreoinstitucionalcontinuasiendoprivada.pdf
[59] Article 3, c) of Data Protection law No. 8968

Public Administration"[60]. Article 9.2. of Data Protection law No. 8968 provides that *"personal data of restricted access, although contained in a public record, are not of unrestricted access as they are of the sole interest of the data subject or the Public Administration. The processing of such data shall be allowed solely for public purposes or with the express consent of the data subject"*.

- Sensitive data: *"information regarding the personal jurisdiction of the individual, such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, socio-economic status, biomedical or genetic information, sexual life and preferences, among others"*[61]. The regime applicable to sensitive data is evaluated in Section II, 10.

- Data regarding Credit Performance: *"Credit performance data shall comply with the National Financial System regulations so as to guarantee financial entities an acceptable level of risk, without hindering the full exercise of the right to self-determination of data or exceed the limits herein"*[62].Article 3, §3 of Executive Decree No. 37554 adds that "*the databases of financial institutions that are subject to control and regulation by the Superintendencia General de Entidades Financieras (SUGEF) do not require registration with the Data Protection Agency of Inhabitants. Notwithstanding the foregoing, the Agency shall have full jurisdiction to regulate and supervise the protection of the rights and guarantees covered under Law No. 8968 and to exercise all the actions granted for this purpose, on said databases".*

By consequence of these provisions, the legal regime regulating personal data is not uniform. The law considers that certain data are subject to more in-depth protection, restricts their processing and therefore the access of third parties to them. Unlike these data, others that appear in public databases of general access are considered unrestricted access. Therefore, there is no particular protection in order to access them:

- Article 2, §2, b) Data Protection law No. 8968 provides that *"Express consent shall not be necessary when [...] these are personal data of unrestricted access, obtained from sources of general public access"*. In the same way, Article 5 of executive decree No. 37554 provides that *"express consent shall not be necessary when [...] it is personal data of unrestricted access, obtained from sources of general public access".*

- Article 26, h) of executive decree No. 37554 provides that the exercise of the right to deletion or elimination is not applicable in the case *"it concerns personal data of unrestricted access, obtained from sources of general public access"*.

The rest of the rules of the Law and the Decree seem to be applicable to personal data of unrestricted access.

4.3. Activities covered by the general legislation

4.3.1. Notion of data processing

[60] Article 3, d) of Data Protection law No. 8968
[61] Article 3, e) of Data Protection law No. 8968
[62] Article 9. 4. of Data Protection law No. 8968

Under Costa Rican law, the notion of "(Personal) data processing" is linked to the notion of "database". In its turn, the concept of "database" refers to the concepts of "automated data processing" and of "file". Furthermore, the legislative framework contains additional definitions concerning "Data in the cloud", "Consultation", "Distribution, dissemination" and "Erasure or Elimination".

"(Personal) data processing" is defined as follows:

- Article 3, i) of Data Protection law No. 8968 defines the notion of "Personal data processing" as being *"any operation or set of operations performed through automated or manual procedures and applied to personal data, such as the collection, recording, organization, storage, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction, among others".*

- Article 2, x) of executive decree No. 37554 defines "Data Processing" as *being "Any operation or set of operations, carried out through automated or manual procedures and applied to personal data, such as collection, registration, organization, preservation, modification, extraction, consultation, use, communication by transmission, broadcast, distribution or any other way that facilitates access to these, collation or interconnection, as well as blocking, deletion or destruction, among others".*

"Database" is defined as follows:

- Article 3, a) of Data Protection law No. 8968 defines the notion of "database" as *"any file, filing system, record or other structured set of personal data subject to automated or manual processing, regardless of its manner of development, organization or access".*

- Article 2, b) of executive decree No. 37554 defines the notion of "database" as being *"Any file, file, registry or other structured set of public or private personal data that is processed, automated or manual, on the site or in the cloud, under the control or direction of a person in charge, any that it is the modality of its elaboration, organization or access".*

"Automated data processing" and "filing system" are defined as follows:

- Article 2, y) of executive decree No. 37554 defines "Automated Data Processing" as being *"Any operation, set of operations or procedures, applied to personal data, carried out through the use of hardware, software, networks, services, applications, on site or in the cloud, or any other technology of the information that allows the collection, registration, organization, conservation, modification, extraction, consultation, use, communication by transmission, dissemination, distribution or any other way that facilitates access to these, collation, or the interconnection, as well as the blocking, deletion or destruction, exchange or digitization of personal data, among others".*

- Article 2, l) of executive decree No. 37554 defines "File" as being *"Any organized set of personal data, whatever the form, purpose or modality of its creation, storage, organization and access".*

"Cloud data", "Consultation", "Distribution, dissemination" and "Erasure or Elimination" are defined as follows:

- Article 2, i) of executive decree No. 37554 defines "Cloud data" as being *"File, file, registry or other structured set of data that is accessed using the Internet"*.

- Article 2, g) of executive decree No. 37554 defines "Consultation" as being a *"Request made to a database, in which specific information is required based on defined search criteria, provided that such request does not result in a database translocation or replica"*.

- Article 2, j) of executive decree No. 37554 defines "Distribution, dissemination" as being *"Any way in which personal data is distributed or published, to a third party, by any means as long as there is an end to commercialize the data or mediate profit with the database"*[63].

- Article 2, u) of executive decree No. 37554 defines "Erasure or Elimination" as the *"Procedure by which the person in charge or the person in charge of the database permanently or partially deletes or destroys the personal data of the owner from its database"*.

4.3.2. Material scope of application

According to Article 2, §1 of Data Protection law No. 8968, the law applies to "*to personal data held in the manual or automated databases of <u>private or public entities</u>, and to any other form of future use of such data"*.

According to Article 3 of executive decree No. 37554, *"This Regulation will be applied to the personal data that appear in the automated or manual databases of <u>public or private organizations</u>, and to any form of subsequent use of these data, as long as they take effect within the national territory, or the Costa Rican legislation derived from the conclusion of a contract or under the terms of international law"*.

4.3.3 Notions of "controller" and "processor"

The Costa Rican framework contains definitions of concepts closely linked to the one of « controller »:

- Article 3, h) of Data Protection law No. 8968 defines « Database controller » as *« a natural or legal person that manages, administrates or is in charge of a database, either public or private, which is competent, as provided by law, to decide the purpose of the database, the personal data categories to be registered and how such data will be processed »*.

- Article 2, s) of executive decree No. 37554 defines « Responsible » as *« Any natural or legal person, public or private, who administers or, manages or is in charge of, or owns,*

[63] j) Distribución, difusión: Cualquier forma en la que se repartan o publiquen datos personales, a un tercero, por cualquier medio siempre que medie un fin de comercializar el dato o medie el lucro con la base de datos.

one or more public or private databases, competent under the Law, to decide which is the purpose of the database, what categories of personal data should be recorded and what type of treatment will be applied to them ».

The Costa Rican Data Protection law No. 8968 does not contain a definition of « processor ».

However, executive decree No. 37554 defines the concept of « Manager » as follows*: « Any natural or legal person, public or private entity, or any other body that processes personal data on behalf of the person responsible for the database ».*

According to article 30 of executive decree No. 37554 entitled « Data processing by the manager »:

> *« The person in charge may only intervene in the treatment of personal databases, as established in the contract concluded with the person in charge and her indications ».*

Article 32 of said Decree specifies the content of a "code of minimum conduct, which shall be transmitted to the processor for full adherence

Furthermore, according to article 31 of said Decree:

> *« The manager will have the following obligations in the treatment of personal databases:*
>
> *a) Only treat personal data in accordance with the instructions of the person in charge;*
> *b) Refrain from processing personal data for purposes other than those instructed by the controller;*
> *c) Implement security measures and comply with the minimum protocols of action in accordance with the Law, this Regulation and the other applicable provisions;*
> *d) Keep confidentiality regarding the personal data processed;*
> *e) Refrain from transferring or disseminating personal data, except express instructions from the person responsible;*
> *f) Delete the personal data object of treatment, once the legal relationship with the person in charge or by instructions of the person in charge has been fulfilled, as long as there is no legal provision that requires the conservation of personal data.*

4.3.4. Activities or organisations excluded by the general legislation(s)

Domestic use exemption

Article 2, §2 of Data Protection law No. 8968 contains a very broad "domestic use exemption" by excluding from its material scope *"the databases carried by any natural or legal person exclusively for internal, personal or domestic purposes, provided such databases are not sold or in any other manner marketed".*

In the same logic, Article 3, §2 of executive decree No. 37554 provides that *"The personal data protection regime established in this Regulation shall not apply to databases maintained by natural or legal persons, public or private, for exclusively internal, personal or domestic purposes, as long as these are not in any way marketed".*

Article 2, c) of executive decree No. 37554 defines “Internal, Personal or Domestic Database” as being *“Any file, file, registry or other structured set of restricted or unrestricted access personal data, maintained by natural persons, will be considered as a personal or domestic database, as long as the databases data or its content is not commercialized, distributed or disseminated. Any file, file, registry or other structured set of personal data maintained by legal entities, public or private, will be considered as an internal database, as long as the databases or their content is not commercialized, distributed or disseminated. They will retain the quality of the internal database”.*

Article 2, j) of executive decree No. 37554 defines “Distribution, dissemination” as being *“Any way in which personal data is distributed or published, to a third party, by any means as long as there is an end to commercialize the data or mediate profit with the database”.*

The concept of “Commercialize” is defined by Article 2, e) of executive decree No. 37554 as being *“Sell, trade, exchange or in any way alienate or pledge, for profit in favor of a third party, one or more times, those personal data that appear in databases”.*

As a result of these different definitions, under Costa Rican law, the domestic exemption is much broader than article 3, §2 of Convention 108+ according to which *“This Convention shall not apply to data processing carried out by an individual in the course of purely personal or household activities”.*

<u>Data of natural persons in their capacity as professionals</u>

Article 3, §4 of Executive Decree No. No. 37554 provides that *“The personal data protection regime established in this Regulation shall not apply to data referring to natural persons in their professional capacity, as long as it is done for the profession's own purposes or in compliance with legal provisions”.*

5. Principle of proportionality

The word “proportionality” does not appear as such in the Law nor in the Decree. The law does not provide for the principle of proportionality to be applied at all stages of the data processing, neither does the law provide for the principle of proportionality to be applied at only some stages of data processing. No recommendations from PRODHAB are to be found to promote compliance with the principle of proportionality at all stages of data processing. However, Article 6 of the Law enounces the principle of data quality, which is examined in Section II, 8.

6. Legitimacy

6.1. Legitimate basis for processing

Under Costa Rican law, consent is the only legitimate basis for the processing of personal data.

Article 5.2 of Data Protection law No. 8968 stipulates that *“Whoever collects personal data must obtain the express consent of the data subject or his representative […].*

Express consent shall not be necessary when:

a) A solid order exists, dictated by a competent legal authority or by agreement adopted by a special investigation commission of the Legislative Assembly in the exercise of its duty.

b) These are personal data of unrestricted access, obtained from sources of general public access.

c) Such data must be surrendered by legal or constitutional order.

Storing data without the informed consent of the individual, or storing data obtained through fraudulent, unfair or unlawful means, is prohibited".

Article 5 of executive decree No. 37554 slightly differs from the Law and provides that: *"Whoever collects personal data must, in all cases, obtain the express consent of the owner for the processing of personal data, with the exceptions established in the Law [...].*

Express consent will not be necessary when:

- *a) There is a well-founded order, issued by the competent judicial authority or an agreement adopted by a special commission of investigation of the Legislative Assembly in the exercise of his office.*
- *b) It is personal data of unrestricted access, obtained from sources of general public access.*
- *c) The data must be delivered by constitutional or legal provision".*

6.2. Notion of consent

Under Costa Rican Law, the notion of consent is closely linked to the obligation to inform data subjects in advance (see Section II, 11 on transparency).

Furthermore, Article 5.2 stipulates that *"consent must appear in writing, either in a physical or an electronic version, and may be revoked in the same manner, but will not have retroactive effects".*

Article 2, f) of executive decree No. 37554 provides for definition of "Consent of the owner of the personal data" as follows: *"Any expression of free, unequivocal, informed and specific wish that is granted in writing or in digital media for a specific purpose, through which the owner of the personal data or his representative, You consent to the processing of your personal data. <u>If consent is granted in the framework of a contract for other purposes, said contract must have a specific and independent clause on consent</u> to the processing of personal data."*

Moreover, Article 4 of executive decree No. 37554 enumerates the requirements for consent as follows:

"Obtaining consent shall be:

a) Free: there must be no error, bad faith, physical or psychological violence or intent, which may affect the owner's expression of will;

b) Specific: referring to one or several determined and defined purposes that justify the treatment;

c) Informed: that the owner has prior knowledge of the treatment, to what their personal data will be subjected and the consequences of giving their consent. Likewise, to know who is responsible for the treatment of your personal data, and their place or means of contact;
d) Unequivocal: it must be granted by any means or through unequivocal conduct by the owner in such a way that its granting can be demonstrated without doubt and that it can be consulted later;
e) Individualized: there must be a minimum of consent given by each owner of the personal data".

Article 5, §§2 and 3 of executive decree No. 37554 list the formalities of consent as follows:

> *"The consent must be granted by the owner, in a physical or electronic document. In the case of consent obtained online, the person responsible must make a procedure available for granting consent in accordance with the Law.*
>
> *Likewise, the document through which the author of the personal data extends his consent, must be easy to understand, free of charge and duly identified".*

Article 6 of executive decree No. 37554 provides that *"In order to demonstrate obtaining consent, the burden of proof will fall, in all cases, on the person in charge of the database"*.

For the specific case of data transfers, also see *infra* Article 14 of the Law and Article 40 of Decree No. 37554.

6.3. Guidelines of PRODHAB

PRODHAB has not issued specific guidelines of general nature on the concept of consent. However, in a press release on the topic of minors[64], the supervisory authority considered that :

> *« Concerning a transfer of data to third parties, it is essential have the express and unequivocal consent of the parents of the minors. This consent must be explicit as to the use and processsing that will be made of the data to be collected from students, and under no circumstances may they be used for any other purpose to the above mentioned ».*

In another press release on the topic of Whatsapp[65], PRODHAB considered that :

> *« In 2014, a Court condemned a man for unauthorized access to his cell phone's text messages wife and a mutual friend. "In that case, both their rights to privacy were violated. The Court found that the husband made an arbitrary and abusive incursion into the privacy of the offended, so that access to a device or to a partner's account*

[64] PRODHAB, Los menores de edad también tienen derecho a proteger sus datos personales, Comunicado de prensa, 08 de septiembre, 2017, available at http://prodhab.go.cr/download/COMUNICADOS/losmenoresdeedadtambientienenderechoaprotegersusdatospersonales.pdf

[65] PRODHAB, ¿Realmente puedo entrar a la cuenta de WhatsApp de un tercero sin su autorización?, Comunicado de prensa, 12 de diciembre, 2017, available at http://prodhab.go.cr/download/COMUNICADOS/RealmentepuedoentraralacuentadeWhatsAppdeuntercerosinsuautorizacion.pdf

without their consent may set up a criminal with prison," said the National Director of PRODHAB, MBA. Wendy Rivera Román. Additionally, this type of practice, which for some may be innocent, transgresses fundamental rights and involve the configuration of serious and very serious offences according to Law No. 8968, of Protection of the Person in front of the Treatment of its Personal Data. According to Article 30, it shall be considered a serious offense "(a) To collect, store, transmit or any other way to use personal data without the informed and express consent of the owner data... c) Collect, store, transmit or otherwise use data personal for a purpose other than that authorized by the owner of the information ».

7. Purpose limitation principle

7.1. Purpose limitation principle and principle of further compatible use

Article 6.4 of the Law provides that:

> *"Personal data shall be collected for specified, explicit and legitimate purposes and shall not be further processed in a way incompatible with such purposes. Further data processing for historical, statistical or scientific purposes shall not be considered as incompatible provided that appropriate safeguards are established to protect the rights herein. Databases may not have purposes contrary to the law or public morals".*

Article 2, w) of Decree No. 37554 defines this principle with relation to "transfer of personal data" as:

> *" Action by which the personal data of the person in charge of a personal database is transferred to any third party other than the person in charge, his economic interest group, the person in charge, service provider or technological intermediary, in these cases as long as the recipient does not use the data for distribution, dissemination or marketing".*

Article 2, n) of Decree No. 37554 defines "Technological intermediary or service provider" as being a*" Natural or legal person, public or private that provides infrastructure, platform, software or other services"*.

Article 14 of the Law contains the general rule applying to data transfers:

> *"Controllers of databases, public or private, may only transfer data contained in such databases <u>with the express and valid authorization of the data subject</u>, without impinging upon the principles and rights provided herein"*.

In addition, article 40 of Decree No. 37554 enumerates the conditions for transfer:

> *« <u>The transfer will always require the unequivocal consent of the owner</u>. The transfer implies the transfer of personal data by the sole and exclusive party of the person responsible who transfers the person responsible for receiving the personal data. <u>Said transfer of personal data will always require the informed consent of the owner, unless otherwise provided by law, also that the data to be transferred has been lawfully collected or collected and according to the criteria that the Law and these Regulations provide</u>. The transfer of personal data of the person in charge of a database to a*

> *manager, service provider or technological intermediary or companies of the same economic interest group is not considered a transfer.*
> *<u>Any sale of data from the file or the database, partial or total, must meet the requirements</u> established in the preceding paragraph ».*

7 .2. Guidelines of PRODHAB

PRODHAB has not issued specific regulations or guidelines, neither of general nature nor for specific fields of processing, to promote compliance with the purpose limitation principle in practice.

7.3. Safeguards applicable to the processing of personal data for historical, statistical and scientific purposes

Article 6.4, §2 of Data Protection law No. 8968 foresees that *« Further data processing for historical, statistical or scientific purposes shall not be considered as incompatible provided that appropriate safeguards are established to protect the rights herein ».*

In addition, article 2, o) of Decree No. 37554 defines « Scientific research » as being the *« Process of applying a scientific method that seeks to obtain relevant and reliable information to understand, verify, correct or apply data, including personal data of a non-sensitive nature or which, being sensitive, are not identifiable, in order to obtain knowledge and solve scientific, philosophical or empirical-technical problems ».*

Read together, these two provisions contain safeguards applicable to the processing of personal data for historical, statistical and scientific purposes. However, the nature of these safeguards are not being detailed for what concerns processing of personal data for historical and statistical purposes. As for the safeguard consisting in anonymizing data for scientific purposes, it only applies to sensitive data.

This being said, in opinion C-123-2012 of the Órgano Superior Consultivo, it was ruled that:

> *"Article 8.d in relation to article 6.4, both of the Law for the Protection of Persons from the Processing of their Personal Data, contemplates the exceptional possibility that the Promotora de Comercio de Costa Rica S.A. transmits - for purposes of subsequent statistical processing - the data related to the information provided in the customs declarations of the exporting companies. This is provided that there is a technical and legal guarantee that there is no risk that persons can be identified.*
>
> *The validity of a transfer made under article 6.4 LPDATA also depends on whether the existence of a public interest is corroborated and that the transfer and subsequent statistical processing of the data are certainly necessary for the fulfilment of the competences of the transferee body".*

Curiously, article 2, r) of Decree No. 37554 contains a definition of « Disassociation procedure » but this concept is not being used in the operative part of the decree. This being said, as an exemption to the general rule according to which personal data may not be « be kept ten years after the date on which the registered facts occurred, unless otherwise provided through special regulatory provisions », article 6.1 of the Law foresees that « in cases where data must be stored for longer periods, they shall be <u>unrelated</u> to the relevant data subject ».

It is also important to note that:

- Article 8, d) of Data Protection law No. 8968 contains an exemption to the Citizen´s Right to Self-determination of Data when the following objective is pursued : *« Operation of databases used for historical, statistical or scientific purposes, provided there is no risk of identifying individuals »*.

- Article 26, e) of Decree No. 37554 contains an exception to the exercise of the right of deletion or elimination in case of *« the operation of databases that are used for statistical, historical or scientific research purposes, when there is no risk that people will be identified »*.

These exemptions will be discussed in Section VI.

8. Data quality principle

8.1. Data quality principle in the legislation

Article 6 of Data Protection law No. 8968 provides that *"Personal data may only be collected, stored or utilized for automated or manual processing when such data are current, truthful, accurate and adequate, considering the purposes for which they were collected".*

In addition:

- Article 6.1 of the Law foresees that: *"Personal data must be kept up to date. The database controller shall eliminate data no longer relevant or necessary for the purposes for which they were received and filed."*

- Article 6.2 of the Law foresees that: *"The database controller shall rectify or erase inaccurate data and shall ensure data are processed fairly and lawfully".*

- Article 6.3 of the Law foresees that: *"Personal data must be accurate. The database controller shall take the necessary measures to ensure that inaccurate or incomplete data, considering the purposes for which they were collected or further processed, are erased or rectified"*

Article 27 of Decree No. 37554 foresees that *« the person in charge of the database must ensure that the principle of information quality is applied »*.

8.2. Guidelines of PRODHAB

PRODHAB has not issued specific regulations or guidelines of general nature to promote compliance with the purpose limitation principle in practice.

However, in a press release on the topic of electronic invoicing[66], the supervisory authority considers that:

[66] PRODHAB, Emisores de factura electrónica deben garantizar la seguridad de los datos de sus clientes, Comunicado de prensa, 16 de Enero, 2019, available at http://prodhab.go.cr/download/COMUNICADOS/Emisoresdefacturaelectronicadebengarantizarlaseguridaddelosdatosdesusclientes.pdf

“To send the invoice customers must provide their full name, ID number and email address. However, there are those who go further and request data such as the phone, physical address or even the license plate number of the vehicle (when it comes to gas station payments). "It is important to emphasize that the business or the person responsible for the database must respect the purpose for which those data are processed, and the customer is entitled to limit himself to providing the data that is strictly necessary” […] The Law 8968 of Protection of the Person from the Processing of its Personal Data and its Regulation, emphasize that personal data can be processed only with the consent of the owner and the person who collects them must be limited to the purpose for which they were requested. Failure to comply with this point and request the data to generate a invoice and then transfer them without permission of the holder to a third party, or use them as a means of contact to offer some service or promotion, is also grounds for economic sanctions”.

Likewise, in a press release relating to possible "tracking" of COVID 19 patients[67], the supervisory authority reminds the information quality principle as follows:

« UP TO DATE: The person responsible for the data will delete the data that have stopped be relevant or necessary, because of the purpose for which they were received and registered. After 10 years, they must be disassociated from its owner. TRUTHFUL: The person responsible for the database is required to modify or delete the data that are not true. Likewise, it will ensure that the data are processed in a loyal and lawful manner. ACCURACY: The person responsible for the data will take the necessary measures to ensure that inaccurate or incomplete data, with with respect to the purposes for which they were collected or for which they were subsequently processed, are deleted or rectified ».

9. Principle of limited retention of personal data

Article 6.1 of Data Protection law No. 8968 provides that:

“The database controller shall eliminate data no longer relevant or necessary for the purposes for which they were received and filed. Personal data that may in any manner affect the data subject shall in no case be kept ten years after the date on which the registered facts occurred, unless otherwise provided through special regulatory provisions. In cases where data must be stored for longer periods, they shall be unrelated to the relevant data subject”.

Article 11 of the Executive Decree adds that:

« The conservation of personal data that may affect the owner, must not exceed a period of ten years, from the date of termination of the data processing object, unless special regulatory provision establishes another term, which by the agreement of the parties is has established a different term, that there is a continuous relationship between the parties or that there is a public interest to preserve the data ».

[67] PRODHAB, Sobre posible “rastreo” de pacientes con COVID-19, Comunicado de prensa 15 de Mayo, 2020, available at http://prodhab.go.cr/download/COMUNICADOS/SobreposiblerastreodeCOVID19.pdf

10. Special categories of personal data

10.1. Notion of sensitive data

Article 3, e) of Data Protection law No. 8968 defines "Sensitive data" as follows:

> *"Information regarding the personal jurisdiction of the individual, such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, socio-economic status, biomedical or genetic information, sexual life and preferences, among others".*

However, article 9, §1 of the Law lists only the following data to be "sensitive":

> *"Personal data revealing racial or ethnic origin, political opinions, religious, spiritual or philosophical beliefs, and the processing of data concerning health, or sexual life or orientation, among others".*

In the above provision, the terms "amongst others" could be considered as creating uncertainty, except if these refer to the categories not listed in article 9, §1 but being mentioned in article 3, e): socio-economic status, biomedical or genetic information.

Compared to article 6 of Convention 108+, the following categories are not listed by the Costa Rican data protection framework:

- trade-union membership;
- personal data relating to offences, criminal proceedings and convictions, and related security measures;
- biometric data uniquely identifying a person.

10.2. Regime applicable to sensitive data

Article 9 of Data Protection law No. 8968 provides that:

> *"No person shall be obliged to provide sensitive data [...].*
>
> *This prohibition shall not apply when:*
>
> *a) Data processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent.*
>
> *b) Processing is carried out in the course of its legitimate activities and with the appropriate guarantees by a foundation, association or any other body with a political, philosophical, religious or trade-union aim, and on condition that the processing relates solely to the members of the body or to persons who have regular contact with the foundation, association or body, in connection with its purposes, and that the data are not disclosed to a third party without the consent of the data subject.*

c) The processing relates to data which are manifestly made public by the data subject or are necessary for the establishment, exercise or defence of legal claims.

d) The processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of health care or medical treatment or the management of health-care services, and where those data are processed by a health care professional, subject to the obligation of professional secrecy, or by another person also subject to an equivalent obligation of secrecy.

10.3. Complementing specific and additional safeguards

Article 37, §2 of Decree No. 37554 foresees that *« In the case of sensitive personal data, when the law allows it, the person responsible must review and, where appropriate, update the corresponding security measures, at least once a year ».*

10.4. Expansion of sensitive data

Neither the Law nor the Decree allow for the special categories of data to be expanded. However, as already mentioned, this depends how the words "amongst others" in article 3, e) of Data Protection law No. 8968 should be interpreted.

10.5. Guidelines of PRODHAB

PRODHAB has interpreted these special categories of data or their regime in several opinions or illustrative cases.

In a press release concerning the distribution of morning pills[68], the supervisory authority considered that:

« In reference to the publications of some medias about the limitations that apparently some pharmacies impose to allow the sale of the "morning after" pill, the PRODHAB reminds the population in general that Law No. 8968 does not allow the processing of personal data considered sensitive. First, it should be clarified that Law No. 8968 of Protection of the Person against the Processing of your Personal Data defines as sensitive data any information concerning the person's private sphere and for which its unauthorized use by the holder could cause some discrimination. The most common are data revealing racial origin, political opinions religious or spiritual beliefs, socioeconomic status, biomedical information, genetics, life and sexual orientation. This regulation states that no person is obliged to provide sensitive data and even prohibits their processing, with some exceptions indicated in the Law ».

In a press release on the processing of COVID-19 patient data[69], the supervisory authority considered that:

[68] PRODHAB, ¡Tenga cuidado con el manejo de datos sensibles!, Comunicado de prensa 24 de septiembre, 2019, available at http://prodhab.go.cr/download/COMUNICADOS/Tengacuidadoconelmanejodedatossensibles.pdf
[69] PRODHAB, Tratamiento de datos de pacientes con COVID-19, Comunicado de prensa 12 de marzo, 2020, available at http://prodhab.go.cr/download/COMUNICADOS/TratamientodedatosdepacientesCOVID19.pdf

« With the arrival of COVID-19 in Costa Rica, popularly known as "Coronavirus", the PRODHAB remembers that the processing of information concerning health is considered sensitive, so it should be carried out in strict compliance with the provisions of Law No. 8968, on the Protection of the Person from the Processing of Personal Data. According to this regulation, there are 4 fundamental aspects to be considered. About disclosing patients' names. According to the Law, the information related to the people, such as biomedical information or genetics, life, among others, is considered sensitive and therefore, no person is obliged to supply it and their processing is prohibited. Some exceptions are cited such as cases where it is necessary to safeguard the vital interest of the person concerned or another person, or is required for the prevention or medical diagnosis, or health care and management, for example. Likewise, it is valid to process sensitive personal data if the person voluntarily made them public. To disclose the name and other data that make a patient identifiable, it is necessary to have the consent of the owner. Otherwise, it should be mentioned only as a statistical data, after anonymization of any personal data. About data handling by professionals of health. The public health facilities, the centers (in case they have the consent of the of the data subject) and health professionals who work in them, may request and transfer between them patient data, as long as it is consistent with all the principles established by Law No. 8968 in its articles 5, 6, 8, 9 and 10. That is, provided that are respected the principle of informed consent and its exceptions, the principle of information quality and security according to the corresponding data categories. In addition, all health officials who have access to this type of data by virtue of its functions, have to comply with the duty of confidentiality and professional secret that covers them, during and after of the processing of a patient's data. Data collection. The Ministry of Health, by virtue of his function, is entitled to process the data of patients carrying COVID-19 or any similar disease ».

11. Transparency principle

11.1. Transparency principle in legislation

Article 5 of Data Protection law No. 8968 provides that:

"*When personal data are requested, data subjects or their representatives shall be notified in advance in a clear, precise and unambiguous manner:*
a) Regarding the existence of a personal database.
b) Regarding the purposes pursued by collecting such data.
c) Regarding the recipients of the information, as well as who may consult such information.
d) Regarding the mandatory or optional nature of their responses to questions that may be posed while collecting such data.
e) Regarding the manner in which the data requested will be processed.
f) Regarding the consequences of refusing to provide the data.
g) Regarding the possibility of exercising their rights.
h) Regarding the identity and address of the database controller.
Such warnings shall appear clearly and legibly when using questionnaires and other means to collect data".

In comparison with article 8 of Convention 108 +, the following information are not to be provided to the data subject:

- the legal basis of the intended processing;
- the categories of personal data processed;
- the means of exercising data subjects' rights.

11.2. Exceptions

Neither the Data Protection law No. 8968 nor the Decree No. 37554 contain any exceptions to the transparency requirements comparable to Article 11 of Convention 108+.

However, the transparency principle is subject to general exemptions to the Citizen´s Right to Self-determination of Data set forth in article 8 of the Law when the following objectives are pursued:

> a) National security.
> b) Security and the exercise of public authority.
> c) Prevention, prosecution, investigation, detention and repression of criminal offences or breaches of ethics in professions.
> d) Operation of databases used for historical, statistical or scientific purposes, provided there is no risk of identifying individuals.
> e) Adequate rendering of public services.
> f) Effective ordinary activities of the Administration performed by official authorities.

These exemptions are examined in Sections III to VI.

11.3. Guidelines by PRODHAB

PRODHAB has not issued specific regulations or guidelines, either of general nature or for specific fields of processing, to promote compliance with the principle of transparency in practice.

12. Principle of security

12.1. Duty of confidentiality

Article 11 of Data Protection law No. 8968 provides that:

> *"<u>The controller, and any person involved in any manner with personal data processing</u>, is subject to a <u>duty of professional secrecy</u> with regard to confidential information to which they have access, even after their connection with the database has ended. The person concerned may be released from his duty of secrecy by judicial decision, in which case only the strictly necessary data, specific to that case, shall be disclosed".*

Article 2, m) of the Decree No. 37554 defines the Guarantee of Confidentiality as being:

> *"Obligation of any natural or legal person, public or private, <u>who has participation in the treatment or storage of personal data</u>, to comply with the duty of confidentiality required by law".*

12.2. Duty of security

Article 10 of the Data Protection law No. 8968 provides that:

> *"The controller shall implement appropriate technical and organizational measures to guarantee the protection of personal data against alteration, accidental or unlawful destruction, loss, unauthorized processing or access and against all other unlawful actions.*
> *Such measures must include, as minimum, the most adequate state of the art physical and logical security mechanisms to protect stored data.*
> *Personal data that do not fully comply with the conditions that guarantee the security and integrity of a database, processing centre, equipment, systems and programs shall not be filed.*
> *Regulations shall describe the requirements and conditions of automated and manual databases and of the persons involved in the collection, storage and use of such data".*

Article 34 of the Decree No. 37554 adds that:

> *"The person responsible must establish and maintain the administrative, physical and logical security measures for the protection of personal data, in accordance with the provisions of the Law and these Regulations. Security measures means the control or group of controls to protect personal data.*
> *Likewise, the person responsible must ensure that the person in charge of the database and the technological intermediary comply with said security measures, to safeguard the information".*

Concerning the "manager", article 31, c) of the Decree No. 37554 provides that he must:

> *"Implement security measures and comply with the minimum protocols of action in accordance with the Law, this Regulation and the other applicable provisions".*

In addition, as already mentioned, Article 31 of the Decree enumerates the obligations of the data processor, amongst which:

> *"c) Implementing the security measures and complying with the codes of minimum conduct pursuant to the Law, these Regulations and other applicable provisions;*
> *d) Maintaining the confidentiality of the personal data processed".*

12.3. Level of security measures and updates

Article 35 of the Decree No. 37554 lists the factors to determine security measures as follows:

> *The person responsible will determine the security measures applicable to the personal data that is processed or stored, considering the following factors:*
> *a) The sensitivity of the personal data processed, in cases that the law allows;*
> *b) Technological development;*
> *c) The possible consequences of a violation for the holders of their personal data;*
> *d) The number of personal data holders;*
> *e) Previous vulnerabilities occurred in the treatment or storage systems;*

f) The risk for the value, quantitative or qualitative, that the personal data could have; and
g) Other factors resulting from other laws or regulations applicable to the person responsible".

In addition, article 37 of said Decree prescribes updates to security measures upon occurrence of specific events, as follows:

> *"Those responsible must update the security measures when the following events occur:*
> *a) The security measures or processes are modified for their continuous improvement, derived from the revisions to the security policy of the person in charge;*
> *b) Substantial modifications in the treatment or storage occur, leading to a change in the level of risk;*
> *c) The technological platform is modified;*
> *d) The systems for processing or storing personal data are violated, in accordance with the provisions of the Law and these Regulations; or,*
> *and) There is an effect on personal data, different from the previous ones.*
> *In the case of sensitive personal data, when the law allows it, the person responsible must review and, where appropriate, update the corresponding security measures, at least once a year".*

12.4. Guidelines of PRODHAB

PRODHAB has published specific guidelines of general nature authored by INTECO (Instituto de normas tecnicas de Costa Rica) to promote compliance with the principle of data security[70].

In this document, INTECO considers *"that it is very important that Costa Ricans are informed and attentive to the security of their data. The INTE/ISO/IEC 27001 standard supports them and helps them to meet this objective".*

12.5. Data breach notification

Article 38 of the Decree No. 37554 foresees that:

> *"<u>The controller shall inform the data subject</u> of any irregularity in the processing or storage of his data, such as loss, destruction, misplacement, among others, resulting from a vulnerability of security or that he learns of, for which he shall have <u>five working days from the moment the vulnerability occurred, so that the affected data subjects can take appropriate measures</u>.*
> *Within the same term, an exhaustive review shall commence to determine the magnitude of the affectation, and the corresponding corrective and preventive actions".*

In addition, article 39 of said decree specifies that:

> *"The controller shall inform the data subject and the Agency, in case of vulnerabilities to security, at least the following:*
> *a) The nature of the incident;*
> *b) The personal data compromised;*

[70] INTECO, Norma técnica garantiza a costarricenses la protección de su información personal contenida en bases de datos, 26 de enero, 2017, available at http://prodhab.go.cr/Comu2017/

c) The corrective actions taken immediately; and
d) The means or place where more relevant information can be obtained".

12.6. Concrete way to notify data breaches

Article 59 of the Decree No. 37554 indicates that:

> *"Proceedings for the protection of rights shall apply when: […]*
> *b. Personal data are collected, stored and transmitted using mechanisms that are not secure or do not guarantee data security and inalterability; […]*
> *i. Personal data are obtained from the data subject or third parties through deceit, violence, willful misconduct, bad faith or threat".*

Concretely, in such cases, in accordance with article 60 of said decree, data subjects can report a data breach by filling this form:

http://www.prodhab.go.cr/download/PROCEPROTDERECHOS/FormulariosProcedimientodeProtecciondeDerechos.docx

13. Individual's rights

13.1. List of data subjects' rights

Article 7 of the Data Protection law No. 8968 enumerates the following rights:

- Right to access;
- Right to rectification, update and erasure.

Article 7 of the Executive Decree No. 37554 provides for a right to revocation of consent.

Article 13 and 24 of the Data Protection law No. 8968 provides for the:

- Right to remedy
- Right to assistance from a supervisory authority

Are not listed nor by the Law nor by the Decree the:

- Right not to be subject to automated individual decisions
- Right to object
- Right to know the reasoning underlying data processing

However, the right to access imposes the report *"to be accompanied by an explanation of the technical terms used"* and the data subject must be *"informed of the system, program, method or process used to process his personal data"*.

13.2. General rules applicable for the exercise of rights

Article 7 of the Data Protection law No. 8968 contains the general rules according to which:

> *"Every individual has the right to access his personal data, to modify or erase these and to consent to the transfer of his data.*
> *The database controller must comply with the request of an individual, <u>free of charge</u>, and <u>must resolve as appropriate within five working days</u> from receiving the request".*

Article 15 of the Decree No. 37554 indicates that:

> *"The rights of access, rectification, modification, revocation or elimination shall be exercised by the data subject or his representative, upon prior accreditation of the ownership or representation".*

Article 16 of the Decree No. 37554 indicates that:

> *"The controller must make available to the data subject, simplified means and forms of electronic communication or others he deems relevant to facilitate the exercise of the rights of the data subjects".*

Article 17 of the Decree No. 37554 indicates that:

> *"The request for access, rectification, modification, revocation or elimination, for the purposes of the Law and this Regulation, must indicate the means for receiving notifications.*
> *In the event this requirement is not fulfilled, the automatic notification established in the Law of Judicial Notifications, Law No. 8687, of 4 December 2008, published in La Gaceta No. 20 of 29 January 2009 and its amendments, shall apply".*

Article 18 of the Decree No. 37554 foresees that:

> *"The controller must process all requests for the exercise of the personal rights of the data subject. The term to address a request shall be five working days, counted from the day following receipt of the request by the controller, in which case he will note the corresponding reception date on the receipt delivered to the data subject.*
> *The term indicated shall be interrupted in the event the controller requires additional information from the data subject".*

Article 19 of the Decree No. 37554 foresees that:

> *"In the event the information provided in the request is insufficient or erroneous to address it, the controller may require from the data subject, for a single time and within the five working days following receipt of the request, that he submit the elements or documents necessary to address it. The data subject shall have a term of five working days counted from the day following receipt to address the requirement.*
> *Should no response be received within said term, the corresponding request shall be considered not to have been presented. In the event the data subject addresses the requirement for information, the term for the data subject to respond to the request shall be five working days, counted from the day following the data subject addressing the requirement".*

Article 22 of the Decree No. 37554 imposes that:

> *"Any controller who rejects addressing any request from a data subject shall justify his response in writing. Should the data subject consider it appropriate, he may bring his case to the Agency, pursuant to Chapter VII "Protection of Rights by the Agency" of these Regulations".*

13.3. Right of access

13.3.1. Right of access in the legislation

Article 7.1 of the Data Protection law No. 8968 provides that:

> *"Data must be stored in such a manner as to fully guarantee the right of access by the data subject.*
> *The right to access personal data guarantees the following powers of the data subject:*
> *a) To obtain at reasonable intervals, as provided in the regulations, without delay and free of charge,* confirmation as to whether or not data relating to him are held *in files or databases. In the event such data exist, these shall be communicated to the data subject in an accurate and intelligible manner.*
> *b) To receive information regarding himself, as well as the purpose of processing, and the use given to such data. The report must be complete, clear and free of codifications. It must be accompanied by an explanation of the technical terms used.*
> *c) To be informed in writing, extensively, through physical or electronic means, of the complete data subject record, even when the request applies only to a portion of said personal data. In no case shall this report disclose third party data, even if related to the data subject, unless when the data will be utilized to accomplish a criminal offence.*
> *d) To be informed of the system, program, method or process used to process his personal data.*
>
> *In the event of data regarding a deceased individual, his successors or heirs shall exercise this right".*

13.3.2. Terms and fees

In addition to the general rules applicable to the exercise of rights detailed in Section 13.2, the following provisions specifically apply to the right of access.

Article 20 of the Decree No. 37554 foresees that:

> *"In all cases, the controller shall respond to requests received from the data subject, regardless of whether his personal data are contained in the database or not, in accordance with the term established in the Law and in these Regulations.*
> *The response by the controller to the data subject shall refer to the totality of the record belonging to the data subject, even if the requirement only encompasses one aspect of the personal data and shall be presented in a legible, understandable and easy to access format. In the event codes, acronyms or keywords are used, the corresponding meanings shall be presented.*
> *This report in no case shall reveal data belonging to third parties, even if linked with the requesting data subject".*

Article 21 of Decree No. 37554 specifies the terms of the exercise of the right to access:

> *"The data subject has the right to obtain from the controller all information related with his personal data, including any pertaining to the conditions, purposes and generalities of their processing.*
> *He may consult the database, with a minimum interval of six months, except if the data subject expresses to the controller, in a well-founded manner, the motives and evidence for which he considers there is a violation of the rights protected in the Law and this Regulation. In the event the controller of the database considers the motives are unacceptable and there is a possibility of an abusive use of said right, within the five working days following the request he shall submit the matter to the PRODHAB, which shall issue a definitive resolution within the term of ten working days following receipt of the submission.*
> *The controller shall address the data consultation within the term of five working days following receipt of the request".*

Article 7 of the Data Protection law No. 8968 indicates that no fees can be requested:

> *"The database controller must comply with the request of an individual, free of charge, and must resolve as appropriate within five working days from receiving the request".*

13.3.3. Guidelines from PRODHAB

The supervisory authority has not issued, on its own initiative, specific guidelines nor regulations, neither of general nature nor for specific fields of processing, to promote compliance with the individual's right of access.

However, PRODHAB has published a template form that can be filled by data subjects to exercise their right to access. This form is available at:

http://www.prodhab.go.cr/download/PROCEPROTDERECHOS/Formularioaccesodatos.docx

13.4. Rights to rectification, update and erasure

13.4.1. Rights to rectification, update and erasure in the legislation

Article 7.2 of the Data Protection law No. 8968 provides that:

> *"The data subject is entitled to, as applicable, the rectification, update or erasure of data the processing of which does not comply with the provisions herein, in particular because of the incomplete or inaccurate nature of the data, or because they were collected without authorization of the data subject.*
> *Any data subject may request and obtain from the database controller the rectification, update, cancellation or erasure, and the fulfilment of the confidentiality guarantee regarding his personal data.*
> *In the event of data regarding a deceased individual, his successors or heirs shall exercise this right".*

Article 23 of the Decree No. 37554 specifies that:

"The owner may request at any time the person responsible to rectify their personal data that turns out to be inaccurate, incomplete or confusing".

Article 25 of said Decree specifies that:

"The owner may request at any time to the responsible, the deletion or total or partial removal of the owner's personal data, permanently".

Article 26 of said Decree specifies that:

"The owner may request at any time to the person responsible, the total or partial deletion or elimination of personal data".

Exemptions to the right of deletion or elimination are examined in Sections III to VI.

13.4.2. Terms and fees

In addition to the general rules applicable to the exercise of rights detailed in Section 13.2, the following provisions specifically apply to the right to rectification.

Article 24 of Decree No. 37554 foresees that:

"The rectification request must indicate what personal data it refers to, as well as the correction that is requested to be made and must be accompanied by the pertinent documentation or proof that supports the origin of the request. The person responsible must offer mechanisms that facilitate the exercise of this right for the benefit of the owner".

13.4.3. Guidelines from PRODHAB

The supervisory authority issued, on its own initiative, specific guidelines for specific fields of processing, to promote compliance with the individual's right to rectification and erasure. This was the case in a press release on the topic of negative credit records deletion[71]. In this document:

"PRODHAB became aware of a company offering to delete negative credit records of the persons at the Superintendencia General de Entidades Financieras (SUGEF), in exchange of an economic amount. According to the user who consulted us, apparently this entity operates as a loan house, and when their customers do not qualify for credit due to their record with SUGEF, they offer them to deposit an amount and complete a form for them to update the information at the Superintendencia when they are subjects of the credit. The form they send to their clients is the same as the Prodhab has enabled on its website www.prodhab.go.cr that in fact anyone can download, complete and submit at no cost to the entity where they need to access, update or delete personal information." In addition to profiting from a document and a procedure that according to Law No. 8968 must be free and personal, it must contain sufficient arguments to clean

[71] PRODHAB, No se deje engañar: no pueden cobrarle por actualizar o eliminar sus datos personales, Comunicado de prensa, 10 de Agosto, 2020, available at http://prodhab.go.cr/download/COMUNICADOS/Nosedejeenganar.pdf

the credit history of the person and claim to give him/her a credit at the end; which clearly can't only be pretentious or wrong, and consists of a possible customer fraud" […] According to Article 7 of Law No. 8968, on Protection of the Person against the Processing of his Personal Data, every person has the right to access his personal data, the rectification or deletion of these and to consent to the transfer of their data. From his side, the person responsible for the database must comply with and resolve the person's request, free of charge, within five working days from the reception of the application. The person who requires to exercise this right, can use the forms provided by Prodhab as a guide, or write their own application and present it directly to the entity where they want to access, update or delete their data. Therefore, we do not think it is necessary to hire third parties to carry out this procedure. It is important to clarify that in Costa Rica the right to forgetfulness in civil matters (for credit operations) is of four years, counted from the date of any of the following situations: that, even if arrears exist, the debt has been formally cancelled, that the same institution that granted the credit to the debtor declared it uncollectible; or that the debt has been declared prescribed by a judicial authority".

Moreover, PRODHAB has published a template form that data subject can fill in order to exercise their right to rectification, update and erasure. This form is available at

http://www.prodhab.go.cr/download/PROCEPROTDERECHOS/FormularioparaejercerelDerechodeRectificacionyoSupresiondeDatosPersonales.docx

13.5. Right to revocation of consent

The Executive Decree No. 37554 organizes the right to revocation of consent as follows:

- *Article 7: "At any time, the owner may revoke their consent to the processing of their personal data, for which the person responsible must establish expeditious, simple and free mechanisms that allow the owner to revoke their consent".*

- *Article 8: "The person in charge of the database, upon presentation of the request for revocation of consent, will have a period of five working days from the receipt of the same, to proceed according to the revocation. Likewise, within the same period of five business days, you must inform those physical or legal persons to whom you have transferred the data of said revocation, which must proceed within five business days from the notification to execute the revocation of the consent.*
  The revocation of consent will not have retroactive effect".

- *Article 9: "When the owner requests confirmation of the cessation of the processing of their data, the person responsible must respond free of charge, expressly within three business days, from the submission of said request".*

- *Article 10: "In case of refusal, express or tacit, on the part of the person in charge, to process the revocation of consent, the owner may submit to the Agency the corresponding complaint referred to in the Law and these Regulations".*

13.6. Right to a remedy

Article 13 of the Data Protection law No. 8968 provides that:

"Data subjects are entitled to a simple and streamlined administrative procedure with the PRODHAB to seek protection against actions that may affect their fundamental rights herein and without detriment to the general or specific jurisdictional guarantees provided by law for this same purpose".

13.7. Right to assistance from a supervisory authority

Article 24 of the of the Data Protection law No. 8968 provides that:

"Any person with a subjective right or legitimate interest may lodge a claim with the PRODHAB, indicating that a public or private database is violating the regulations or basic principles for protection of data and the right to self-determination of data established herein".

Article 58 of the Executive Decree No. 37554 foresees that:

"Any person who has a subjective right or a legitimate interest can denounce, before the Agency, that a public or private database acts in contravention of the rules or basic principles for data protection and informative self-determination, established by the Law and these Regulations.
Likewise, the Agency may automatically initiate a procedure to verify whether a database is being used or not, in accordance with the Law and these Regulations".

14. Additional obligations

14.1. Obligation to respect the accountability principle

Article 27 of the Decree No. 37554 provides that:

"The controller shall establish and document procedures for the inclusion, conservation, modification, blocking and erasure of personal data, on site or in the cloud, based on codes of minimum conduct and security measures in the processing of personal data. In addition, the controller of the database shall be responsible for applying the principle of data quality".

In addition, article 36 of Decree No. 37554 foresees that:

"In order to establish and maintain the physical and logical security of the personal data, the controller shall undertake as minimum the following actions, which may be required at any time by the Agency:
a) Develop a detailed description of the type of personal data processed or stored;
b) Create and maintain an updated inventory of the technological infrastructure, including the equipment and computer programs and their licenses;
c) Indicate the type of system, program, method or process used in data processing or storage [...];

14.2. Registration requirement for some databases

Article 21 of the Data Protection law No. 8968 provides that:

> *"All databases, public or private, processed for purposes of distribution, dissemination or marketing must register with the registry established by the PRODHAB. Registration does not imply data diversion or transfer.*
> *All information foreseen in legal regulations and in the codes of conduct […] must be filed."*

Article 2, j) of Decree No. No. 37554 defines "Distribution, dissemination" as being: "*Any way in which personal data is distributed or published, to a third party, by any means provided that there is a purpose to commercialize the data or mediate profit with the database".*

The concept of "marketing" is defined by Article 2, e) of executive decree No. 37554 as being *"Sell, trade, exchange or in any way alienate or pledge, for profit in favor of a third party, one or more times, those personal data that appear in databases".*

Article 44 of the Decree No. No. 37554 lists the information to be provided when registering a database.

Finally, according to article 78 of the Decree No. No. 37554:

> *"Pursuant to the Law, all databases, public or private, aimed at distribution, dissemination or marketing, must register with the Agency and pay the Agency the sum of two hundred dollars of the United States of America (USD $200.00), at the highest sale exchange rate of reference as determined by the Central Bank of Costa Rica on the date such payment is made. This sum is the annual database regulation and administration fee".*

The link to the list of registered databases is currently broken, see:
http://www.prodhab.go.cr//Bases-de-Datos/?inscritas

Processing personal data without being registered with the PRODHAB is considered as a gross offence under article 31, e) of the Law.

Article 28, c) of the Law provides*: "For gross offences, a fine of fifteen to thirty base salaries of a Court Assistant I, pursuant to the National Budget Law, and a suspension of one to six months in the utilisation of the personal data filing system"*.

14.2. Data protection impact assessment obligation

Article 36 of Decree No. 37554 imposes that:

> *"In order to establish and maintain the physical and logical security of the personal data, the controller shall undertake as minimum the following actions, which may be required at any time by the Agency: […]*
> *d) Develop a risk analysis, which consists of identifying hazards and estimating the risks that may affect the personal data;*

e) Establish the security measures applicable to the personal data, and identify those effectively implemented;
f) Calculate the existing residual risk based on the difference between the existing security measures and those not in existence that may be necessary for the protection of the personal data;
g) Develop a work plan for the implementation of the missing security measures, based on the result of the calculation of the residual risk".

This being said, it should be noted that PRODHAB has no power to approve the result of risk analyses carried out by controllers. Indeed, in a note of August 2020[72], PRODHAB considers that:

"The national director of the Costa Rican Data Protection Agency (Prodhab), sent a letter to Congresswoman Silvia Hernández Sánchez, President of the Special Investigation Commission of UPAD, clarifying a statement made by systems engineer Esteban Jiménez during his appearance in the Legislative Assembly on July 30th.
Jiménez was summoned to appear as an expert in relation to the transfer of data that was handled in principle from the National System of Information and Unique Registry of State Beneficiaries (SINIRUBE).
According to the document sent by Mora, when referring to the impact analysis, the expert would have indicated that this analysis should have been carried out by a competent body that approved the project, specifically Prodhab.
According to the head of Prodhab, this declaration gave rise to later statements in the press indicating that in order for "the SINIRUBE database to be transferred to the private association Horizonte Positivo, the responsible institution must have complied with a previous procedure before Prodhab" so that "it could authorize the transfer of this data, based on national legislation.
However, the director of Prodhab maintains that in the existing and current national legislation, there is no procedure like the one described, nor is it considered a figure that resembles the concept of impact analysis.
"Although the general European regulations contemplate this figure, and at the international level impact analysis is spoken of as a good practice for the treatment of personal data, it is incorrect to say that for a data transfer to take place in Costa Rica, this procedure must be complied with, since as is reiterated, there is no regulation that regulates it," stated Mora.
The office also points out that agreements for the transfer of personal data are the exclusive responsibility of the person responsible for the database, in accordance with article 3, paragraph h, of Law No. 8968 on the Protection of Individuals with regard to the Treatment of their Personal Data. And that it is said responsible for the database, who must adopt all the security measures established by the regulations in its article 10, and the guarantor of having the unequivocal consent of the owner, as indicated in article 40 of the Regulations of the Law.
"It is not appropriate for this Agency to approve or give its approval to a figure such as the impact analysis, since the Law does not contemplate this figure, and therefore, even less so for this Agency to make revisions or approvals in this respect", concludes the document".

[72] See https://www.facebook.com/notes/agencia-de-protecci%C3%B3n-de-datos-de-los-habitantes-prodhab/prodhab-aclara-a-comisi%C3%B3n-investigadora-de-upad/3194512480632806/

14.3. Specific technical and organizational measures provided by Law

Article 12 of the Data Protection law No. 8968 provides that

> *"Any natural and legal person, public and private, in charge of the collection, storage and use of personal data may draw up codes of conduct establishing the appropriate steps to collect, store and manage personal data, pursuant to the regulations herein.*
> *In order to be deemed valid, such codes of conduct, and any further modifications thereof, must be registered with the PRODHAB. The PRODHAB may, at any time, verify that the database is in full compliance with the terms set out in its code.*
> *Data processed under a code of conduct registered with the PRODHAB will be presumed, iuris tantum, compliant with the provisions herein in order to authorize transferring database contents".*

14.4. Adapted obligations according to the nature and volume of the data, the nature, scope and purpose of the processing

Article 35 of the Decree No. 37554 provides that:

> *"The controller shall determine the security measures applicable to the personal data processed or stored, considering the following factors:*
> *a) The sensitivity of the personal data processed, in the cases allowed by law;*
> *b) The technological development;*
> *c) The possible consequences for the data subjects of a violation of the personal data;*
> *d) The number of personal data subjects;*
> *e) Previous vulnerabilities that occurred in the processing or storage systems;*
> *f) The risk for the quantitative or qualitative value that the personal data may have; and*
> *g) Other factors arising from other laws or regulations applicable to the controller".*

15. International transfers

Neither the Law, nor the Decree contains a section dedicated to international transfers.

Article 31, f) of the Law considers to be a gross offence "*To transfer personal data of Costa Rican citizens or foreigners established therein to third countries without the consent of the data subjects*".

Note that the rules governing "transfers to third parties" apply cumulatively. (See Section II, 7)

Section III - Necessary and proportionate exceptions provided by law for national security and defense purposes (article 11, §1,a & §3)

Exceptions for national security and defense purposes

Article 8 of Data Protection law No. 8968 provides that:

> *"The principles, rights and guarantees set forth herein may be restricted in a fair and reasonable manner in accordance with the principle of administrative transparency when the following objectives are pursued:*

a) National security.
b) Security and the exercise of public authority […]".

Article 14 of executive decree No. 37554 provides that:

> *"The exercise of the rights mentioned in the previous article may be restricted for reasons of national security, public order […], in the cases and with the scope provided in the applicable laws, by duly founded and motivated resolution of the competent authority".*

Article 26 of executive decree No. 37554 provides that:

> *"The data subject may request from the controller at any time the complete or partial elimination or erasure of his personal data, except in the following cases:*
>
> *a) State security; […]*
> *c) Public safety and the exercise of public authority […]".*

It is not clear whether PRODHAB is competent for independent and effective review and supervision of processing activities carried out for national security and defense purposes. Indeed, the above-mentioned exemptions apply to the exercise of rights, principles but also to "guarantees". The extent of the word "guarantees" has not been interpreted in guidelines or communications issued by the supervisory authority.

The Costa Rican authorities have not provided to the Council of Europe any specific legislative texts applying to processing activities carried out for national security and defense purposes. No such legislative text has been identified by the author of this report. Hence, it remains questionable whether exceptions for national security and defense purposes are provided for by law, respect the essence of fundamental rights and freedoms, constitute a necessary and proportionate measure in a democratic society and that they are used lawfully in relation to only a limited number of provisions of the law in line with article 11 of Convention 108 +.

Section IV - Necessary and proportionate exceptions provided by law for other major legitimate interests of the State (article 11, §1,a)

1. Exceptions for other major legitimate interests of the State

Article 8 of Data Protection law No. 8968 provides that:

> *"The principles, rights and guarantees set forth herein may be restricted in a fair and reasonable manner in accordance with the principle of administrative transparency when the following objectives are pursued: […]*
>
> *e) Adequate rendering of public services.*
> *f) Effective ordinary activities of the Administration performed by official authorities".*

Article 26 of executive decree No. 37554 provides that:

> *"The data subject may request from the controller at any time the complete or partial elimination or erasure of his personal data, except in the following cases: [...]*
>
> *b) The data must be kept pursuant to a constitutional or legal provision or by resolution of a judicial entity;*
> *f) Adequate rendering of public services;*
> *g) Effective ordinary activity of the Administration by official authorities".*

The author of this report has not identified any guidelines nor communications in which PRODHAB or another institution has interpreted these exemptions.

2. Exceptions for the protection of important economic and financial interests

No such exemptions have been identified by the author of this report. However, it should be noted that:

- Article 9.4 of Data Protection law No. 8968 specifies that: *"Credit performance data shall comply with the National Financial System regulations so as to guarantee financial entities an acceptable level of risk, without hindering the full exercise of the right to self-determination of data or exceed the limits herein".*

- Article 3, §3 of executive decree No. 37554 adds that *"The databases of financial entities that are subject to control and regulation by the General Superintendence of Financial Entities (SUGEF), will not require registration with the Agency for Data Protection of Inhabitants. Notwithstanding the foregoing, the Agency shall have full jurisdiction to regulate and supervise the protection of the rights and guarantees covered under Law No. 8968 and to exercise all the actions granted for this purpose, on said databases".*

3. Exceptions for the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties

3.1. Exemptions foreseen in the legislation

Article 8 of Data Protection law No. 8968 provides that:

> *"The principles, rights and guarantees set forth herein may be restricted in a fair and reasonable manner in accordance with the principle of administrative transparency when the following objectives are pursued [...]:*
>
> *c) Prevention, prosecution, investigation, detention and repression of criminal offences or breaches of ethics in professions" [...].*

Article 14 of executive decree No. 37554 provides that:

> *"The exercise of the rights mentioned in the previous article may be restricted for reasons of public order [...] or to protect the rights of third parties, in the cases and*

with the scope provided in the applicable laws, by duly founded and motivated resolution of the competent authority".

Article 26 of executive decree No. 37554 provides that:

"The data subject may request from the controller at any time the complete or partial elimination or erasure of his personal data, except in the following cases: […]

d) Prevention, prosecution, investigation, detention and repression of criminal offenses, or breaches of professional ethics; […]".

3.2. Main legal bas/es for exceptions for the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties

Article 8 of the General Law of Police of 1994 (Law No. 7410 of 1994, 26 May 1994) provides that:

"These are general powers of all police forces […]:

l) Keep the necessary record books, which shall include: the police operations, the persons responsible for those activities, the complete list of the personnel involved in each operation, patrol or police action, the personal data, the hours of entry and exit of the detainees, as well as other data that serve for the adequate control of those operations"

Article 24 of the Constitution guarantees the right to intimacy, freedom and secret of communications (See Section II, 2.2). In addition, the following laws should be mentioned.

The Law Against Organized Crime of July 22, 2009[73] governs judicial and procedural investigations in matters of national and international organized crime. The law establishes rules for the interception of private communications and sets forth the obligation of public and private entities to cooperate with the Judicial Centre for the Interception of Communications and judicial authorities conducting criminal investigations. Failing to do so could result in the cancellation or revocation of their respective concession title or licence pursuant to the General Telecommunications Law (Law No. 8642 of 4 June 2008).

According to article 14 of the Law Against Organized Crime - Judicial Center for the Intervention of Communications:

"The Judicial Branch will be in charge of the Judicial Center for Communications Intervention (CJIC), with the necessary personnel to operate twenty-four hours a day, every day. This unit will perform the intervention of communications ordered by criminal judges throughout the country, when to do so it is possible to use the technology available. Each year, the person who is the President of the Supreme Court of Justice, in a private session, shall inform the Ministers of the Presidency, Justice, Public Security and Government, to the Public Prosecutor's Office and the OIJ, about the efficiency, effectiveness and results of the Judicial Center for the Intervention of Communications, as well as improvements to be made for updating".

[73] Ley Contra la Delincuencia Organizada, No. 8764.

Article 15 of the Law Against Organized Crime - Intervention of communications:

> *"In all investigations undertaken by the Public Prosecutor's Office for organized crime, the court may order, by means of a reasoned decision, the intervention or listening of communications between present or by the epistolary, radial, telegraphic, telephonic, electronic, satellite or any other means. The procedure for the intervention will be that established by Law No. 7425, Search, seizure and examination of private documents and intervention of communications. The time of the intervention or listening can be up to twelve months, and can be renewed by an equal period, with the prior authorization of the judge".*

Article 16 of the Law Against Organized Crime lists the major crimes for the investigation of which intervention of private communications including the use of electronic means may be carried out.

Power of national tribunals to authorize the registry, seizure or the analysis of any private document including e-mail communications when it may be deemed necessary in order to clarify criminal matters under their jurisdiction is regulated by Law No. 7425 of 1994 on Search and Seizure of Documents and Intervention on Private Communications[74].

The obligation of internet service providers and telecommunications companies to facilitate cooperation with judicial authorities for the intervention of private communications through the Judicial Centre of Intervention of Communications and to enforce the measures ordered by competent judges is regulated by article 20 of Law No. 7425 of 1994 and articles 14 and 17 of the Law No. 8754 Against Organized Crime.

Article 20 of Law No. 7425 of 1994 provides that:

> *"The companies and institutions that provide communication services are obliged to grant, to the judicial authority, all the material and technical facilities so that the interventions are effective, safe and confidential.*
> *In order to inform them about the judicial disposition, it will be necessary to receive an official letter from the Court, in which the necessary information is stated; it will not be a requirement to notify them of the content of the resolution that ordered the measure".*

3.3. Specialized institutions

The Judicial Investigation Organism of Costa Rica has a Division on Cybercrime Investigations, which along with the corresponding Offices of Public Prosecutors pertaining to the Ministerio Publico are the main authorities in charge of the investigation of crimes, including crimes committed through the use of computer systems and Internet.

The Computer Security and Incident Response Team (CSIRT-CR) of the Ministry of Science, Technology and Telecommunications, which was officially created in March 2012 is the official government entity that facilitates and coordinates matters on information security and cybercrime among government entities and financial institutions pertaining to the State. The CSIRT-CR is composed of the heads of the main national Ministries and is the entity in charge of facilitating support and cooperation with administrative and judicial authorities for the

[74] Ley sobre registro, secuestro y examen de documentos privados e intervencion de las comunicaciones, No.7425 de 09 de agosto de 1994.

investigation and prosecution of cybercrime and the coordination of activities and tasks within the Inter-American Committee Against Terrorism (CICTE) of the Organization of the American States and with Interpol.

3.4. Criminal record database

Article 40 of Law No. 5524 (Organic Law of the Judicial Investigation Body) provides that:

> *"The Criminal Archive will be in charge of an expert in the field. It will have the files and other documents, duly classified, of all persons who at any time have appeared before the authorities as allegedly responsible for punishable acts, and also those sent by national or foreign authorities".*

In June 2019, article 41 of Law No. 5524 was amended by bill 20997[75] as follows:

> *"All information contained in the Criminal File must have a confidential nature and will be for the use of the Agency, the Directorate of Intelligence and Security (DIS) and the following police departments that make up the Ministry of Public Security: the Police Drug Control (PCD), the Public Force (FP), National Coast Guard (SNG), Air Surveillance Service (SVA),Directorate of Border Police (Difro), General Directorate of Armament (DGA), the Directorate of Private Security Services (DSSP), Professional Police of Migration and Foreigners".*

The aim of this modification was to making it easier for the police forces to take better prevention by having the necessary inputs and background information of persons under investigation[76].

4. Exceptions for other essential objectives of general public interest

Article 26 of executive decree No. 37554 provides that

> *"The data subject may request from the controller at any time the complete or partial elimination or erasure of his personal data, except in the following cases:*
>
> *h) These are personal data of unrestricted access, obtained from sources of general public access".*

For further details about this exemption, read Section II, 4.2.

<u>Section V - Necessary and proportionate exceptions provided by law for major interests of private parties (article 11, §1, b)</u>

1. Exceptions for the protection of the data subject

The author of this report has not identified such exemptions.

[75] See http://www.asamblea.go.cr/glcp/doc_relevantes_de_actas/Dictamen%2020.997.pdf
[76] See http://www.aselex.cr/boletines/Proyecto-20997.pdf

2. Exceptions for the protection of the rights and fundamental freedoms of others

Article 14 of executive decree No. 37554 provides that:

> *"The exercise of the rights mentioned in the previous article may be restricted for reasons of [...] public health provisions or to protect the rights of third parties, in the cases and with the scope provided in the applicable laws, by duly founded and motivated resolution of the competent authority".*

The author of this report has not identified guidelines of PRODHAB about this exemption.

Section VI - Restrictions on the rights and additional obligations for data processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes (article 11, §2)

Exceptions for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

Article 8 of Data Protection law No. 8968 provides that:

> *"The principles, rights and guarantees set forth herein may be restricted in a fair and reasonable manner in accordance with the principle of administrative transparency when the following objectives are pursued [...]:*
>
> *e) Operation of databases used for historical, statistical or scientific purposes, provided there is no risk of identifying individuals. [...]".*

Safeguards applicable to the processing of personal data for historical, statistical and scientific purposes are discussed in Section II, 7.3.

Section VII - Other Sectoral Data Protection Law and codes of conduct

Lex specialis and codes of conduct

Article 42 of the General Telecommunications Law No. 86423 guarantees the privacy of communications and protection of personal information as follows:

> *"The operators of public networks and providers of publicly available telecommunications services must guarantee the secrecy of communications, the right to privacy and the protection of personal data of subscribers and end users, by implementing the necessary systems and technical and administrative measures. These protection measures shall be established by regulation by the Executive Branch.*
>
> *Operators and suppliers must adopt the appropriate technical and administrative measures to guarantee the security of the networks and their services. In case the operator knows of an identifiable risk in the security of the network, it must inform Sutel and the end users about such risk.*

The operators and suppliers must guarantee that the communications and the traffic data associated to them, will not be listened to, recorded, stored, intervened or monitored by third parties without their consent, except when the corresponding judicial authorization has been obtained, in accordance with the law".

Article 43 of said Law provides that:

"Traffic and location data relating to end users that are processed and stored under the responsibility of an operator or provider must be deleted or made anonymous when not required for the purpose of transmission of a communication or the provision of a service.

Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed until the expiry of the period during which the bill may legally be challenged or payment demanded.

Location data may be processed only if made anonymous or with the consent of subscribers or users, to the extent and for the time necessary for the provision of a service".

There is a complementary administrative regulation Nº 35205-MINAET that guarantees the secrecy of communications, the right to privacy, and the protection of personal data of subscribers and users.

The author of this report has not identified other lex specialis nor codes of conduct.

Section VIII - Supervision & Enforcement

1. Ensuring effective and independent oversight

1.1. Establishment of a supervisory authority

Article 15 of Data Protection law No. 8968 provides that:

"A maximum de-concentration entity is created, attached to the Ministry of Justice and Peace, with the name of Agencia de Protección de Datos de los Habitantes (Inhabitant Data Protection Agency - PRODHAB). It shall have its own legal identity to perform the duties assigned to it herein and manage its own resources and budget, and may sign contracts and agreements as necessary to perform its duties. The Agency <u>shall enjoy independence</u> to emit judgement".

1.2.Independence and confidentiality

Article 17 of Data Protection law No. 8968 provides that:

"PRODHAB management shall consist of a national director with at least a Bachelor´s degree in a related subject matter and a well-known professional and moral background.

An owner, shareholder, board member, manager, advisor, legal representative or employee of a personal data collection or storage firm shall not be appointed as national director. This prohibition shall continue two years after leaving such position. Likewise, the spouse or relative up to third degree of kinship or affinity of a person holding the abovementioned positions is banned from assuming such position".

Article 18 of Data Protection law No. 8968 provides that:

"PRODHAB shall have the necessary technical and administrative staff to adequately perform its functions, appointed upon suitability contest, pursuant to the Civil Service Bylaws or as established by the relevant regulations. The staff must keep professional secrecy and confidentiality with regard to confidential data to which they may have had access during the exercise of their functions".

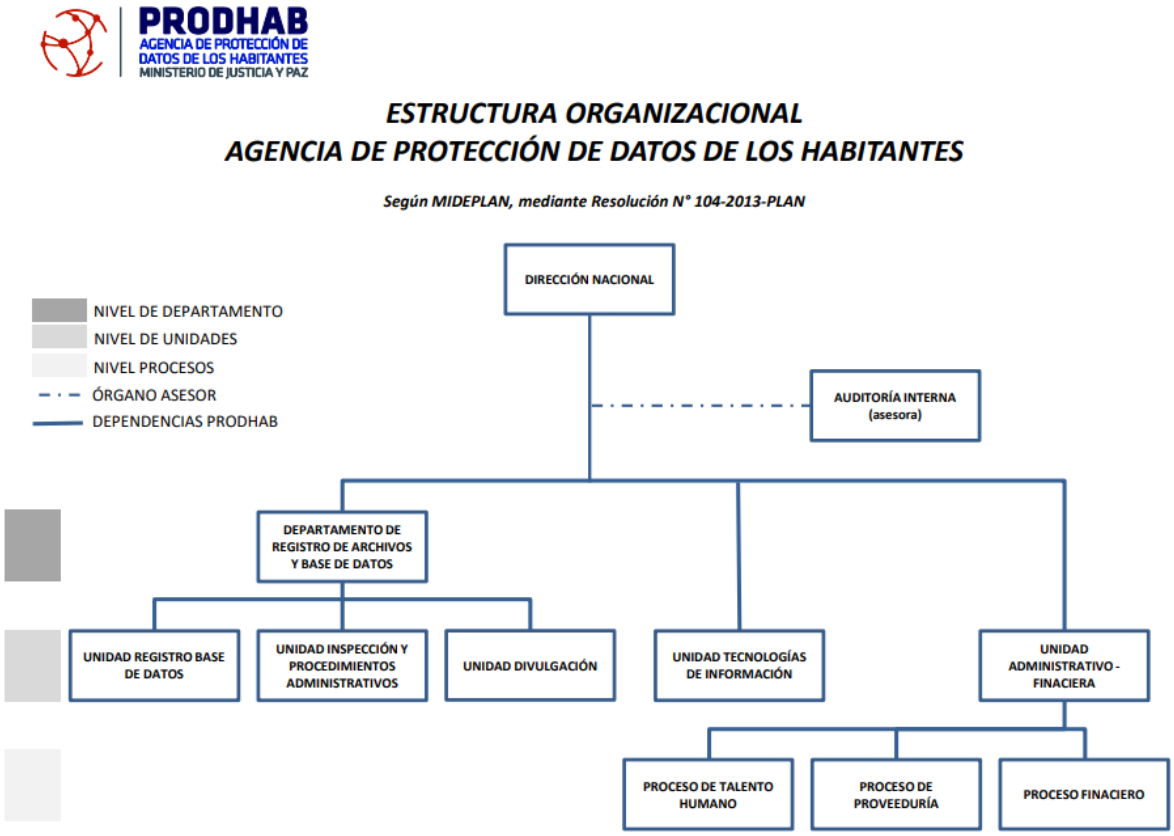
Article 19 of Data Protection law No. 8968 specifies that:

"The following prohibitions apply to all PRODHAB employees:
a) Rendering services to persons or firms dedicated to personal data collection, storage or handling. This prohibition shall continue two years after leaving such position.
b) Becoming interested, personally and unduly, in Agency information.
c) Disclosing, or in any manner disseminating, personal data to which they have access on occasion of their position. This prohibition shall continue indefinitely even after their employment has ended.
d) Exercising their profession externally while holding a professional position in the Agency. This does not apply to academic activities in higher education centres or the liberal practice in favour of relatives up to third degree of kinship or affinity, provided the assumption in paragraph a) is not met.
Breach of any provision above shall be deemed gross misconduct with regard to the application of the disciplinary regime, without detriment to other applicable liabilities".

1.3. Management and staff

On the website of PRODHAB, the following organizational description of the supervisory authority is to be found[77]:

[77] See https://drive.google.com/file/d/0B2xTi4E2qWBqM1BHR20xbmx4czA/view



According to PRODHAB's website[78]:

> *"The organizational structure presented above is the one approved by Mideplan, however, to date it does not have its own internal audit and who currently exercises these functions is the internal audit of the Ministry of Justice and Peace.*
>
> *Additionally:*
>
> *The Head of the Administrative-Financial Unit has not been created.*
> *In relation to the Archives and Database Registry Department, the Database Registry units and the Inspection and Administrative Procedures unit in practice operate as a single unit. Due to the nature of its functions, the Disclosure unit depends directly on the National Directorate".*

The occupational structure, updated as of May 2020 can also be found on PRODHAB's website[79]:

[78] See http://prodhab.go.cr/recursoshumanos/
[79] See https://drive.google.com/file/d/1etXCuoweUrS50N0MMJuJKYwQ4Q_LC3Jq/view

PRODHAB
AGENCIA DE PROTECCIÓN DE DATOS DE LOS HABITANTES
MINISTERIO DE JUSTICIA Y PAZ

AGENCIA DE PROTECCIÓN DE DATOS DE LOS HABITANTES
ESTRUCTURA OCUPACIONAL

Nombre Funcionario	Genero	Puesto	Clase del Puesto	Especialidad
DIRECCIÓN NACIONAL				
MORA ELIZONDO ELIZABETH	F	504206	DIRECTOR NACIONAL	No cuenta con ninguna especialidad
UNIDAD ADMINISTRATIVO - FINANCIERO				
BARRANTES FONSECA MARIO ALONSO	M	509086	PROFESIONAL DE SERVICIO CIVIL 2	ADMINISTRACIÓN DE RECURSOS HUMANOS
*VACANTE	M	509087	PROFESIONAL DE SERVICIO CIVIL 2	ADMINISTRACIÓN GENERALISTA
FONSECA CORTÉS RENE RAFAEL	M	366559	PROFESIONAL DE SERVICIO CIVIL 2	ADMINISTRACIÓN DE NEGOCIOS
CALVO SÁNCHEZ DOUGLAS	M	509088	PROFESIONAL DE SERVICIO CIVIL 2	CONTABILIDAD
UNIDAD TECNOLOGÍAS DE INFORMACIÓN				
HERNANDEZ PORRAS SALATIEL	M	509089	PROFESIONAL EN INFORMÁTICA 2	INFORMÁTICA Y COMPUTACIÓN
SOSA ARIAS YAHAIRA ROCIO	F	509090	PROFESIONAL EN INFORMÁTICA 1-C	INFORMÁTICA Y COMPUTACIÓN
CASCANTE SEGURA MANUEL	M	509091	PROFESIONAL EN INFORMÁTICA 1-C	INFORMÁTICA Y COMPUTACIÓN
DEPARTAMENTO DE REGISTRO DE ARCHIVO Y BASE DE DATOS				
QUESADA RODRÍGUEZ KARLA	F	509094	PROFESIONAL JEFE DE SERVICIO CIVIL 1-B	DERECHO
SALAZAR GÓMEZ DOUGLAS GERARDO	M	509085	PROFESIONAL DE SERVICIO CIVIL 2	DERECHO
LÓPEZ MORA MARÍA ALJANDRA	F	509092	PROFESIONAL DE SERVICIO CIVIL 1-B	DERECHO
AMADOR LÉPIZ MANUEL ENRIQUE	M	060090	PROFESIONAL DE SERVICIO CIVIL 2	DERECHO
UNIDAD DE DIVULGACIÓN				
BARBOZA BARBOZA TATIANA MARÍA	F	509093	PROFESIONAL DE SERVICIO CIVIL 1-B	PERIODISMO

NOTA: * El propietario se encuentra con actualmente nombrado en un ascenso interino en otra institución.

Actualizado al 19/05/2020

Article 85 of the Decree No. 37554 provides that:

> *"The Data Protection Agency will be under the Public Employment Regime and excluded from the Civil Service Regime, being empowered to incorporate administrative, technical and professional personnel who meet the needs of the public service.*
> *To become a creditor of this Regime under the principle of proven suitability, a public contest must be held, for which the tests determined by the Agency must be carried out and approved".*

Article 86 of the Decree No. 37554 details that:

> *"After conducting the public competition and in order to manage human resources according to needs and promote the administrative career, the Agency will be empowered to carry out internal, extended internal, external competitions, interim appointments or other mechanisms that may guarantee the functioning of the Institution".*

Article 87 of the Decree No. 37554 specifies that:

> *"The Agency must have job position manuals. The Agency shall ensure they are kept updated".*

The descriptive job position manual, as updated in 2019, can be found on PRODHAB's website: https://drive.google.com/file/d/1EAlFaV4rVdhLDclO-6uxtiKFXnz7yczz/view

Article 88 of the Decree No. 37554 regulates the recruitment and selection process as follows:

> *"The recruitment and selection process must have the following phases:*

a) Recruitment: Based on the requirements of the job and position manuals and the Agency's personnel needs, the requirements of each required position will be defined and published. Recruitment can be done both internally and externally to the Agency. Likewise, a register of eligible persons will be established for each position, which will be made up of grades from highest to lowest.
b) Selection: The Agency will define the methodologies, tests, tools and selection criteria that it considers appropriate to apply for the selection of personnel.
c)Conformation of triads or payrolls: They will be conformed according to the position of the participants within the registry of eligible, being able the Agency to choose any of the people who integrate them.
All human resource management and administration processes applied by the Agency must comply with the generally accepted technical standards in this area".

Article 89 of said Decree adds that:

"All Agency staff will be subject to a trial period of up to six months".

1.4. Budget

Article 20 of Data Protection law No. 8968 provides that:

"The PRODHAB budget shall result from:
a) Fees, charges and other duties resulting from the exercise of their functions;
b) Transfers from the State to the Agency;
c) Donations and grants from other governments, national public institutions or international organisations, provided they do not compromise the independence, transparency and autonomy of the Agency;
d) The financial resources generated from the Agency´s own activity.
The amounts from fines established herein shall be used to update PRODHAB hardware and software.
The Agency shall comply with the principles and responsibilities set forth in Titles II and X of Law No. 8131, Law on Financial Administration of the Republic and Public Budgets of 18 September 2001. It must also provide information as may be requested by the Ministry of Finance for its studies. In all other particulars, the scope and enforcement of this Law do not apply to the Agency. Regarding oversight, the Agency shall only comply with the provisions established by the General Comptroller of the Republic".

Concerning the annual budget of PRODHAB, the following documents are available on the authority's website:

- The annual purchasing plan (a document prepared by each unit and that summarizes the investments made by PRODHAB)[80];

- The details of the annual personal's wages[81].

[80] See https://drive.google.com/file/d/1LZBT8Z4pqKYAHixUuBv9cyvI9--Glyxk/view
[81] See https://drive.google.com/file/d/1V82KZFP2cdoyj8vDM1PARkXWo312O4Rc/view

1.5.Annual report

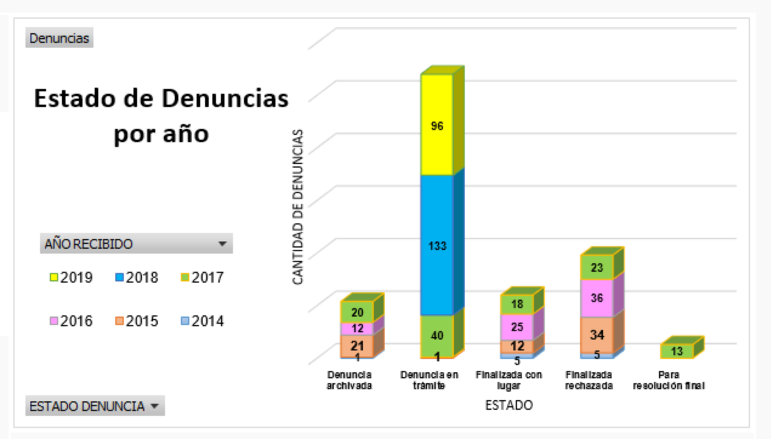
The author of this report has not identified the existence of an annual activity report.

1.6. Complaints

According to PRODHAB's website, in 2019, 96 complaints were handled:

Estado de denuncias por año

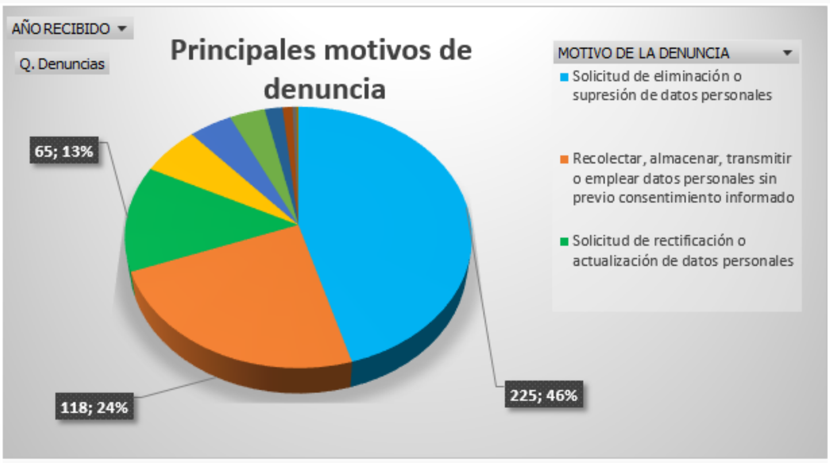
Denuncias	Ingreso						
Estado	2014	2015	2016	2017	2018	2019	TOTAL
Denuncia archivada	1	21	12	20			54
Denuncia en trámite		1		40	133	96	270
Finalizada con lugar	5	12	25	18			60
Finalizada rechazada	5	34	36	23			98
Para resolución final				13			13
TOTAL	**11**	**68**	**73**	**114**	**133**	**96**	**495**



The overall main motives for complaints are the following:

Principales motivos de denuncia

AÑO RECIBIDO	(Todas)
Principales motivos denuncias	**Q. Denuncias**
Solicitud de eliminación o supresión de	225
Recolectar, almacenar, transmitir o empl	118
Solicitud de rectificación o actualización	65
Otros	30
Recolección, almacenamiento y transmis	22
Solicitud de acceso a la información	18
Recolectar, almacenar, transmitir o empl	9
Solicitud de derecho al olvido	5
Robo de datos personales (sensibles o r	2
Acceso a datos personales sin consentir	1
Total general	**495**



The overall distribution of complaints by sector is the following:

Sector denunciado	Denuncias
Banca y finanzas	132
Varios	59
Comercial	56
Gestionadora de cobro	56
Buró de crédito	30
Gobierno	28
Persona física	22
Telecomunicaciones	19
Salud	17
Bufete/ Firma jurídica	15
Cooperativa	13
SD	13
Medio de comunicación	8
Superintendencia/ Entidad Reguladora	7
Administrador página web y/o app	5
Colegio profesional	3
Seguros	3
Tecnología	3
Fundación/ ONG/ ORG	2
Turismo	1
Bienes Inmuebles	1
Educativo	1
Asociación solidarista	1
TOTAL	**495**

A Report of complaints received by type and by year from the2014 as of 06/30/2020 is available here: https://drive.google.com/file/d/1I-gQyxDHkjMgytBfvsJYTNzjktujIP1_/view

There have been some critics about PRODHAB's work to which the agency answered in a press release dating from July 2020[82].

[82] PRODHAB, Editorial de la dirección nacional, 21 de Julio 2020, available at http://prodhab.go.cr/download/COMUNICADOS/Editorialdeladireccionnacional.pdf

1.7. Publication of decisions

PRODHAB’s decisions are not being published. Indeed, when trying to reach the respective section of PRODHAB’s website, the following screen appears:

1.8 Means of challenge

Article 71 of Decree No. 37554 provides that:

> *“Against the final act of the procedure, the filing before the Agency of the ordinary appeal for reconsideration proceeds within the third business day after the respective notification”.*

Article 72 of said Decree adds that:

> *“The appeal for reconsideration, must be resolved by the Agency within eight business days after its presentation”.*

2. Promoting compliance with data protection law, dealing with requests and complaints

2.1. Public awareness raising activities

Article 16 of Data Protection law No. 8968 provides that:

> *“PRODHAB has the following powers, besides others as provided in this and other rules: […]*
> *i) Develop the necessary guidelines for their publication in the official journal La Gaceta to ensure that public institutions implement the appropriate personal data*

processing procedures, while being respectful of the different levels of functional independence and administrative autonomy.
j) Encourage inhabitants to be informed about their rights regarding the collection, storage, transfer and use of their personal data".

PRODHAB issues press releases on specific topics to promote public awareness on the rights of data subjects and on the responsibilities of controllers. These are available at: http://www.prodhab.go.cr/comunicados/

Furthermore, PRODHAB has active accounts on Facebook[83] and Twitter[84] through which the authority conducts campaigns to promote data protection awareness.

The author of this report did not identify any survey results on the level of public awareness.

PRODHAB has given specific attention to the data protection rights of children in a press release of September 2017[85]. In this document, PRODHAB considers that:

"This is a vulnerable population, we all have the obligation to protect them, by not doing so we put at risk your fundamental right and even your physical integrity and that of the rest of the core family," said the MBA. Wendy Rivera, National Director of the Agency. "We urge institutions to approach PRODHAB, we are in the greatest disposition to provide them with free training on the protection of personal data of minors, according to Law 8968. It is also a priority sector, since the Agency is reviewing its compliance in order to carry out the ex officio information requests that correspond".

2.2. System to receive complaints from individuals

Regardless of their nationality, residence or address, the system is made available to individuals to submit complaints which can be found on PRODHAB's website: http://www.prodhab.go.cr/procedimientosdeprote/

It consists into a form[86] that must be filled to submit a complaint to PRODHAB.

According to PRODHAB's website, additional requirements are:

1. Carry identification document at the time of filing the complaint.
2. The evidence that is considered pertinent to demonstrate the denounced facts.
3. As many copies of the complaint and its evidence as there are parties reported in the procedure.
4. Indicate the exact physical address of the party (s) denounced (s).
5. The documents must be presented at the Prodhab offices, duly signed by the complainant.

[83] See https://www.facebook.com/prodhab/
[84] See https://twitter.com/Prodhab_CR
[85] PRODHAB, Los menores de edad también tienen derecho a proteger sus datos personales, Comunicado de prensa 08 de septiembre, 2017, available at http://prodhab.go.cr/download/COMUNICADOS/losmenoresdeedadtambientienenderechoaprotegersusdatospersonales.pdf
[86] See http://www.prodhab.go.cr/download/PROCEPROTDERECHOS/FormulariosProcedimientodeProtecciondeDerechos.docx

3. Powers of supervisory authority(ies)

3.1. Investigation and intervention powers

Article 16 of Data Protection law No. 8968 provides that:

> *"PRODHAB has the following powers, besides others as provided in this and other rules:*
> *a) Ensure compliance with data protection regulations by any private natural or legal person as well as by public entities and bodies.*
> *b) Carry a record of databases regulated under this law.*
> *c) Require controllers to provide the necessary information to perform its duties, including the codes of conduct used.*
> *d) Access the databases regulated herein to ensure effective compliance with personal data protection regulations. This power applies to concrete cases brought to the Agency and, exceptionally, in the event of evidence of violation of overall database or data system management.*
> *e) Settle claims regarding violations to personal data protection regulations.*
> *f) Order, on its own account or upon request of a party, the erasure, modification, addition or restricted circulation of information in files or databases when they contravene personal data protection regulations.*
> *g) Impose the sanctions under Article 28 herein to any natural or legal persons, public or private, that breach personal data protection laws, and report possible related criminal offences to the Public Ministry […]".*

Article 25 of said Law adds that:

> *"[…] At any time, the PRODHAB may order the accused person to submit the necessary information and may perform on-site inspections of such databases or files. To protect the data subject's rights, the Agency may order, by justified decision, precautionary measures to ensure the effective outcome of the process […].*

3.2. Consultation powers

Article 16 of Data Protection law No. 8968 provides that:

"PRODHAB has the following powers, besides others as provided in this and other rules: […] h) Promote, and contribute to drafting, regulations for the implementation of personal data protection regulations".

The author of this report could not identify whether the consultation of PRODHAB by the Legislative Assembly is mandatory.

3.3. Supervision of international transfers

Neither the Law, nor the Decree contains a section dedicated to international transfers (see Section II, 15). Hence PRODHAB has no supervision powers with this regard.

4. Sanctions and remedies mechanisms

4.1. Available remedies mechanisms to data subjects

Article 24 of Data Protection law No. 8968 foresees that:

> *"Any person with a subjective right or legitimate interest may lodge a claim with the PRODHAB, indicating that a public or private database is violating the regulations or basic principles for protection of data and the right to self-determination of data established herein".*

Article 58 of the Decree No. No. 37554 adds that:

> *"Any person who has a subjective right or a legitimate interest can denounce, before the Agency, that a public or private database acts in contravention of the rules or basic principles for data protection and informative self-determination, established by the Law and these Regulations.*
> *Likewise, the Agency may automatically initiate a procedure to verify whether a database is being used or not, in accordance with the Law and these Regulations.*
> *The Agency in the processing of the data protection procedure, will apply the principles established in the Second Book of the General Law of Public Administration".*

4.2. Sanctions enumerated in the legislation

Article 27 of Data Protection law No. 8968 lays down the procedure relating to administrative sanctions, as follows:

> *"The PRODHAB may, on its own account or upon request of a party, open a procedure to verify whether a database under this law is being used according to its principles. In order to comply with this, the PRODHAB must follow the steps established in the General Public Administration Law for the ordinary procedure. A request for reconsideration of the final decision may be requested within three days of its issuance, and a reply must be provided within eight days of receiving such request".*

Article 28 of Data Protection law No. 8968 lists the possible sanctions, as follows:

> *"The following sanctions apply to the offences provided herein, without detriment to other applicable criminal sanctions:*
> *a) For minor offences, a fine of five base salaries of a Court Assistant I, pursuant to the National Budget Law.*
> *b) For serious offences, a fine of five to twenty base salaries of a Court Assistant I, pursuant to the National Budget Law.*
> *c) For gross offences, a fine of fifteen to thirty base salaries of a Court Assistant I, pursuant to the National Budget Law, and a suspension of one to six months in the utilisation of the personal data filing system".*

The minor, serious and gross offences are defined in article 29 to 30 of Data Protection law No. 8968.

In addition, article 70 of the Decree No. 37554 foresees that:

> *"In addition, the Agency may impose written warnings on those actions or omissions that violate the rights enshrined in the Law and these Regulations".*

Finally, article 32 contains possible sanctions regarding public databases, as follows:

> *"When a public database controller commits any of the offences above, PRODHAB shall order the relevant measures to cease or correct any effect thereof. This decision shall be informed to the database controller, the entity such controller works for and the affected parties, if any. The decision may be issued by the Agency on its own account or upon request of a party. This applies without detriment to any applicable criminal liability".*

4.3. Use of sanctions by PRODHAB

The author did not identify any report concerning the use of sanctions by PRODHAB.

Section IX - General context of the evaluation process

Duty to contribute to the evaluation process

See the introduction of this report.