National Assembly

Law No. 03/2016

Protection of Personal Data

Preamble

The relevance of private life, or rather the right to personal data protection, is now an acquisition that is stabilizing in the regional and international level, with an impact in almost every country in the world.

The relationship between the identification data and the life of its bearers is close, and elements such as: name, telephone number, e-mail address, etc., allow anyone, relying on modern technological means, to accept the privacy of third parties for different purposes.

São Tomé and Príncipe, as a State that belongs to the global community, affirms, through this Diploma , the principle that shows that the private life should be protected, without prejudice to the most varied advantages derived from the circulation of personal data. Therefore, it emphasizes the existence of a legal framework linking these two vectors.

In accordance with the changes inherent in the process of socio-economic development, in compliance with the provisions of the Constitution of the Republic and other juridical instruments used in São Tomé and Príncipe, this Diploma establishes the conditions which the use of personal data is permitted and the terms which those responsible for the processing of such data and the holders thereof may proceed for the purpose of guaranteeing rights and obligations.

This Law establishes three relevant guidelines for the processing of personal data, the circulation of such data and, finally, liability arising from non-compliance of the protection obligations.

Firstly, the authorization of the holder and the narrow situations of necessity are enshrined as fundamental requirements for the processing of personal data.

Secondly, the transfer of personal data to a location outside the national territory will depend on theguarantee of protection conferred by this legal system.

Third, all those who, do not accomplish this legal provision, will be responsible for the non-protection of the personal data to which they have access, being subject to both the sanctions provided herein and the contained in other laws to which it refers.

Chapter I

General provisions

Article 1

Object

This Law aims to guarantee and protect the personal data of individual persons.

Article 2

General principles

The treatment of personal data must be processed in a transparent manner and in strict respect for the privacy of private and family life, as well as for the fundamental rights, freedoms and guarantees established in the Constitution of the Democratic Republic of São Tomé and Príncipe, in the instruments of international law and current legislation.

Article 3

Scope of application

1. This Law applies to the processing of personal data by automated means total or partially as well as processing by non-automated means of personal data contained in or intended for use in manual files.

2. This Law is also applied to the processing of personal data carried out:

a) By the controller for treatment of personal data in São Tomé and Príncipe;

b) Within the scope of the activities of the controller established in São Tomé and Príncipe, even if the person is not living in the national territory;

c) Outside of the national territory, where the legislation of Sao Tome and Principe is applicable under public or private international law;

d) For those responsible for the treatment that is not established in São Tomé and Príncipe, use for the processing of personal data, means located in the national territory.

3. For the purposes of paragraph 2 (d), the controller shall have recourse to means situated in the territory of Sao Tome and Principe when the processing of personal data is carried out using the means situated in the national territory, or when personal data are stored in media located in São Toméan territory, based on the purposes of this Law, the use of such means is for the collection, registration or transit of personal data in the national territory.

4. In case of paragraph 2 (d), the controller shall designate, through a communication to the National Agency for the Protection of Personal Data (NAPPD), a representative established in São Tomé and all their rights and obligations, without prejudice to their own responsibility.

5. This Law does not apply to the processing of personal data carried out by a singular person in the exercise of exclusively personal or domestic activities, unless it is intended for systematic communication or diffusion.

6. This Law applies to video surveillance and other forms of capture, treatment and diffusion of sounds and images that allow the identification of persons whenever the controller is living or working in São Tomé and Príncipe or uses a provider of access to networks established in the country.

7. This Law applies to the processing of personal data with the purpose of public security, without prejudice to the provisions of special rules contained in instruments of international law and interregional agreements to which São Tomé and Príncipe is bound and of specific laws related to that sector and others co-related.

Article 4

Definitions

1. For the purposes of this Law, the following in defined as:

a) Personal data: any information, , including sound and image, relating to an identified or identifiable person (data holder); must be identified directly or indirectly, in particular by reference to an identification number or to one or more specific elements of their physical, physiological, psychological, economic, cultural or social identity;

b) Data holder: the person to whom the data subject to treatment relates;

c) Processing of personal data: any operation or operations relating to personal data, whether carried out with or without automated means, such as collection, registration, organization, preservation, adaptation or alteration, retrieval, consultation, use, communication by transmission, dissemination or otherwise making available, by comparison or interconnection, as well as blocking, elimination or destruction;

d) Personal data file: any structured set of personal data, accessibility according to certain criteria, regardless of the form of mobility of its creation.

e) Controller: the singular or legal person, public authority, service or any other body which, individually or jointly with another person, determines the purposes and means of processing personal data;

f) Subcontractor: the individual or legal person, the public authority, the service or any other organism treating the personal data on behalf of the person responsible for the processing;

g) Third party: means the individual or legal person, public authority, service or any other organization that is not acting like the data holder, the controller, the processor or other person directly under the controller or the subcontractor, is authorized to process the data;

h) Recipient: a singular or legal person, a public organism, a service or any other body to whom personal data are disclosed, irrespective of whether or not it is a third party, without prejudice to the authorities to whom information is given in the framework of a legal provision or regulatory provision of an organic nature.

i) Consent of the data holder: means any manifestation of free will, specific and informed, under which the holder accepts that his personal data are processed;

j) Data interconnection: a form of processing consisting in the possibility of relating the data of a file with the data of a file or files held by another controller or others or held by the same controller with another goal;

k) Regulatory provision of an organic nature: a provision contained in a diploma of organization and operation or of a statutory body competent to perform acts of data processing and other acts referred to in this Law.

2. For the purposes of subparagraph e) of the preceding paragraph, where the purposes and means of processing are determined by legal provision or organic regulatory provision, the person responsible for processing the personal data must be indicated.

Chapter II
Data processing

Section I
Quality of personal data

Article 5
Quality of data

1. Personal data must be:

a) Treated lawfully and with due respect for the principle of good faith and for the general principles set out in Article 2;

b) Collected for specified, explicit and legitimate purposes and directly related to the exercise of the activity of the controller, and cannot be further processed in a manner incompatible with those purposes;

c) Appropriate, relevant and not excessive in relation to the purposes for which they are collected and subsequently processed;

d) Accurate and, where necessary, updated, taking appropriate measures to ensure that inaccurate or incomplete data are deleted or rectified, taking into account the purposes for which they were collected or for which they are subsequently processed;

e) Preserved in such a way as to enable the holders to be identified only for the period necessary for the purpose of collecting or further processing.

2. On request of the data controller, and in the case of a legitimate interest, the National Agency for the Protection of Personal Data may authorize the retention of data for historical, statistical or scientific purposes for a period exceeding that referred to in previous number

Article 6

Conditions of legitimacy of data processing

The processing of personal data may only be carried out if the holder has unequivocally authorized it or if the processing is necessary to:

a) Execution of contracts or contracts in which the data holder is a party or prior to the formation of the contract or declaration of negotiation will be made at his request;

b) Compliance with legal obligation to which the controller is facing;

c) Protection of vital interests of the data holder, if he is physically or legally incapable of giving his consent;

d) Execution of a mission of public interest or in the exercise of the powers of a National Agency for the Protection of Personal Data in which the controller is invested or a third party to whom the data are communicated;

e) Pursuit of the legitimate interests of the data controller or third party, to whom the data are disclosed, provided that the interests or rights, freedoms and guarantees of the data subject are not prevailed.

Article 7

Treatment of sensitive data

1. The processing of personal data relating to philosophical or political beliefs, membership of a political or trade union association, religious belief, private life and racial or ethnic origin, as well as the processing of data relating to health and sex life, including genetic data.

2. The processing of the data referred to in the preceding paragraph may, however, be carried out provided that with guarantees of non-discrimination and with the safety measures provided for in article 16, under the following conditions:

a) By legal provision or regulatory provision of an organic nature that expressly authorizes the processing of the data provided for in the previous number; or

b) Authorization of the National Agency for the Protection of Personal Data, when for reasons of important public interest this treatment is indispensable to the exercise of the attributions and competences of its responsible; or

c) Where the data holder has explicitly authorized such treatment.

3. The data referred to in paragraph 1 may also be processed where one of the following conditions is met:

a) Be necessary to protect the vital interests of the data subject or another person and the data subject is physically or legally unable to consent;

b) Be carried out, with the consent of the proprietor, by a legal person or a non-profit-making body of a political, philosophical, religious or trade-union nature, in the course of his legitimate activities, provided that the treat- the members of the body or persons with whom it maintains regular contacts connected with its purposes and that the data are not communicated to third parties without the consent of the holders;

c) It relates to data which are manifestly made public by the holder, provided that consent to the processing of the declarations can legitimately be deduced from his statements;

d) It is necessary for the declaration, exercise or defense of a right in judicial process and is carried out exclusively for that purpose.

4. The processing of data relating to health and sex life, including genetic data, may be carried out where necessary for the purposes of preventive medicine, medical diagnosis, medical care or treatment or management of health services, provided that the processing of such data is carried out by a health professional bound by secrecy or by another person also subject to professional secrecy, is notified to the National Agency for the Protection of Personal Data in accordance with Article 21 and is guaranteed by appropriate information security measures.

Section II
Legitimacy of processing of personal data

Article 8
Suspects of illegal activities, criminal offenses and administrative offenses

1. The establishment and maintenance of central records relating to persons suspected of unlawful activities, criminal offenses, administrative offenses and decisions imposing penalties, security measures, fines and ancillary sanctions may only be maintained by public services with specific competence pre- in view of the legal provision or regulatory provision of an organic nature and observing current procedure and data protection standards.

2. The processing of personal data relating to suspected illegal activities, criminal offenses, administrative offenses and decisions imposing penalties, security measures, fines and

ancillary sanctions may be carried out subject to compliance with data protection and information security standards , where such processing is necessary for the fulfillment of the legitimate purposes of the person responsible, provided that the rights, freedoms and guarantees of the data subject are not prevailing.

3. The processing of personal data for the purpose of police investigation shall be limited to what is necessary for the prevention of a specific danger or repression of a specific offense for the exercise of powers provided for in a legal provision or regulatory provision of an organic nature and even under the terms of an international law instrument or interregional agreement to which São Tomé and Príncipe is bound.

Article 9

Interconnection of personal data

1. The interconnection of personal data that is not provided for in a legal provision or regulatory provision of an organic nature is subject to the authorization of the National Agency for the Protection of Personal Data requested by the responsible or jointly by the corresponding controllers, in accordance with the terms of no. Article 22 (1).

2. The interconnection of personal data shall comply with the following requirements:

a) Suits the pursuit of the legal or statutory purposes and legitimate interests of those responsible for the treatments;

b) Does not lead to discrimination or diminution of the rights, freedoms and guarantees of data holders;

c) Be surrounded by appropriate security measures; and

d) Take into account the type of data subject to interconnection.

Chapter III
Rights of the data holders

Article 10
Right to information

1. When collecting personal data directly from the holder, the controller or his representative must be unless known to him, provide him with the following information:

a) The identity of the controller and, where appropriate, his representative;

b) Purposes of treatment;

c) Other information, such as:

i. The recipients or categories of recipients of the data;

ii. The obligatory or optional nature of the response and the possible consequences if it does not respond;

iii. The existence and conditions of the right of access and rectification, provided that they are necessary, taking into account the specific circumstances of the data collection, to ensure that the data subject is treated in a fair manner.

2. The documents that serve as the basis for the collection of personal data must contain the information contained in the previous number.

3. If the data are not collected from the holder, and unless known, the data controller or his representative shall provide the information provided for in paragraph 1,at the time of registration of the data or, if communication to third parties is foreseen, until the first communication of such data.

4. In the case of data collection in open networks, the data shall be informed, unless he is aware of it, that his personal data may circulate in the network without security, at the risk of being seen and used by unauthorized third parties.

5. The obligation to provide information provided for in this article may be waived in the following cases:

a) By legal provision;

b) For reasons of security and prevention or criminal investigation;

c) where, in particular in the case of the processing of data for statistical, historical or scientific research purposes, the data subject's information proves to be impossible or involves disproportionate efforts or where the law or administrative regulation expressly determines the registration of the data or its disclosure, in which case the National Agency for the Protection of Personal Data should be notified.

6. The obligation to provide information in accordance with the provisions of this Article shall not apply to the processing of data made for exclusively journalistic purposes or for artistic or literary expression in respect of the fundamental rights of the data holder as provided for in paragraph 3 of the following article.

Article 11

Right of access

1. The data holder shall have the right to obtain from the controller free and unrestrictedly at reasonable intervals and without undue delay or excessive costs:

a) confirmation of whether or not data are being processed concerning him, and information on the purposes of such processing, the categories of data concerned and the addressees or categories of recipients to whom the data are communicated;
b) the communication, in an intelligible form, of its data subject to processing and any available information on the origin of such data;

c) Knowledge of the reasons underlying the automated processing of data concerning him;

d) The rectification, elimination or blocking of data whose processing does not comply with the provisions of this Law, in particular due to incomplete or inaccurate data;

e) Notification to third parties to whom the data have been communicated of any rectification, erasure or blocking effected under the terms of the preceding subparagraph, unless this is demonstrably impossible or involves a manifestly disproportionate effort, and third parties to the rectification, erasure, destruction or blocking of data.

2. In the case of the processing of personal data relating to security and to criminal prevention or investigation, the right of access shall be exercised through the competent authority in the case.

3. In the case provided for in no. 6 of the preceding article, the right of access is exercised through the National Agency for the Protection of Personal data with due regard for the applicable norms, namely those that guarantee freedom of expression and information, freedom of the press and the independence and professional secrecy of journalists.

4. In cases referred to in paragraphs 2 and 3, where the communication of the data to its holder is liable to prejudice security, crime prevention or investigation or freedom of expression and information or freedom of the press, the competent authority competent authority in the case or the National Personal Data Protection Agency, respectively, merely inform the data older only of the steps taken that are not liable to prejudice the values that are intended to be safeguarded in this paragraph.

5. The right of access to information on health data, including genetic data, shall be exercised through a physician chosen by the data holder.

6. In cases where data are not used to take action or decisions in relation to specific persons, the law may restrict the right of access in cases where there is clearly no danger of breach of the rights, freedoms and guarantees of the holder of data, in particular the right to privacy, and that data are used exclusively for the purpose of scientific research or are kept in the form of personal data for a period which does not go beyond what is necessary for the sole purpose of producing statistics.

Article 12

Right of opposition

1. Unless otherwise provided by law, the data holder has the right of opposition at any time, for weighed and legitimate reasons relating to his particular situation, to the data subject , in the event of justified opposition, the processing carried out by the person in charge may no longer have such data.

2. The data holder also has the right of request, and free of charge, to the processing of personal data concerning him by the controller for the purposes of direct marketing or any other form of commercial solicitation, or to be informed before personal data are first communicated to third parties for the purpose of direct marketing or used on behalf of third parties and to expressly have the right to oppose such communications or uses without charge.

Article 13

Right of non-subjection to automated individual decisions

1. Any person shall have the right not to be subject to a decision having an effect on his or her legal situation or affecting it in a meaningful way solely on the basis of automated data processing to assess certain aspects of his or her personality, in particular their professional capacity, their credit, the confidence they deserve or their behavior.

2. Without prejudice to compliance with the other provisions of this Law, a person may be subject to a decision taken pursuant to paragraph 1 if it is:

a) taken in connection with the conclusion or performance of a contract, and on condition that his request for the conclusion or performance of the contract has been satisfied, or that there are appropriate measures to safeguard his legitimate interests, in particular his right of representation and expression;

b) Authorized by law that establishes measures that guarantee the protection of the legitimate rights and interests of the data holder.

Article 14
Right to compensation

1. Any person who has suffered damage as a result of unlawful processing of data or of any other act in breach of a legal or regulatory provision concerning the protection of personal data shall have the right to obtain compensation from the controller for the damage suffered.

2. The controller may be partially or totally exonerated from this responsibility if he proves that the act causing the damage cannot be attributed to him.

Chapter IV
Security and confidentiality of treatment

Article 15
Treatment safety

1. The controller shall implement appropriate technical and organizational measures to protect personal data against accidental, unlawful destruction, accidental loss, unauthorized alteration, dissemination or access, in particular where the treatment entails their transmission over a network, and against any other form of unlawful treatment, and must ensure, in the light of the available technical knowledge and the costs resulting from its application, an adequate level of safety in relation to the risks presented by the treatment and the nature of the data to be protected.

2. The controller shall, in the event of processing on his behalf, choose a subcontractor which offers sufficient guarantees in respect of technical security measures and the organization of the processing to be carried out, and shall ensure compliance with those measures.

3. Subcontracting operations shall be governed by a contract or legal act which binds the subcontractor to the controller and stipulates, in particular, that the subcontractor acts only on the instructions of the controller and that it shall also fulfill the obligations referred to in paragraph 1.

4. The evidence of the negotiation declaration, contract or legal act relating to data protection, as well as the requirements relating to the measures referred to in paragraph 1, shall be recorded in a document with probative value which is legally recognized.

Article 16

Special safety measures

1. The data controllers referred to in Articles 7 (2) and8 Shall take appropriate measures to:

a) Prevent access by unauthorized persons to the facilities used for the processing of such data (control of entry to the premises);

b) Prevent data carriers from being read, copied, altered or removed by an unauthorized person (control of data sup- ports);

c) Prevent unauthorized entry and unauthorized disclosure, unauthorized alteration or deletion of personal data (insertion control);

d) Prevent automated data-processing systems from being used by unauthorized persons through data transmission facilities (monitoring of use);

e) Ensure that authorized persons can only access the data covered by the authorization (access control);

f) Ensure the verification of entities to whom personal data may be transmitted through data transmission facilities (transmission control);

g) Ensure that the personal data entered when and by whom (control of introduction) can be recorded, within a period appropriate to the nature of the treatment, to be laid down in the regulations applicable to each sector;

h) Prevent the data from being read, copied, altered or disposed of in an unauthorized manner (transport control) in the transmission of personal data and in the transport of its carrier.

2. Taking into account the nature of the entities responsible for the processing and the type of installations in which it is carried out, the National Agency for the Protection of Personal Data may waive the existence of certain security measures, provided that respect is shown rights, freedoms and guarantees of data holders.

3. The systems shall ensure the logical separation of data on health and sex life, including genetic data, from other personal data.

4. The National Agency for the Protection of Personal Data may stipulate that in cases where the personal data network referred to in Article 7 may jeopardize the rights, freedoms and guarantees of the respective holders, the transmission shall be encrypted.

Article 17
Subcontractor treatment

Any person who, acting under the authority of the controller or the processor, and the subcontractor himself, has access to personal data, may not process it without instructions from the controller, except under legal obligations.

Article 18
Professional secrecy

1. Persons responsible for the processing of personal data, as well as persons who, in the performance of their duties, are aware of the personal data processed shall be bound by professional secrecy even after the end of their duties.

2. Officials, agents or technicians acting as advisory or advisoryProtections of Personal data have to keep the same obligation of professional secrecy.

3. The provisions of the previous numbers do not exclude the obligation to provide mandatory information, in accordance with the law, except when it is contained in files organized for statistical purposes.

Chapter V
Transfer of personal data to a place outside the Democratic Republic of Tome and Principe

Article 19
Principles

1. The transfer of personal data to a place outside the national territory can only be carried out in compliance with the provisions of this Law and if the legal order to which they are transferred ensures a suitable level of protection.

2. The adequacy of the level of protection referred to in the preceding paragraph shall be assessed in the light of all the circumstances surrounding the transfer or the set of data transfers, taking into account in particular the nature of the data, the purpose and the duration of the processing or planned treatments, the countries of origin and of final destination, the general or special rules of law in force in the legal system concerned, as well as the professional rules and security measures which are respected in that same order .

3. The National Agency for the Protection of Personal Data shall be responsible for deciding whether a legal system ensures an adequate level of protection in accordance with the provisions of the preceding paragraph.

Article 20
Derogations

1. The transfer of personal data to a legal system which does not ensure an adequate level of protection pursuant to paragraph 2 of the previous article may be made, by means of notification to the National Personal Data Protection Agency, if the holder of the data has unequivocally authorized for the shipment or where any of the following situations occurs:

a) It is necessary for the execution of a contract between the data holder and the person responsible for processing procedures for the formation of the contract, decided upon at the request of the data holder;

b) It is necessary for the execution or conclusion of a contract concluded or to be concluded, in the interest of the data holder, between the controller and a third party;

c) It is required or required by law to protect an important public interest, or to declare, exercise or defend a right in a judicial proceeding;

d) It is necessary to protect the vital interests of the data holder;

e) It is carried out on the basis of a public register which, according to the law or administrative regulation, is intended to inform the public and is open to consultation with the general public or any person who can prove a legitimate interest, provided that the conditions established for the consultation are fulfilled in the specific case.

2. Without prejudice to paragraph 1, the National Agency for the Protection of Personal Data may authorize a transfer or set of transfers of personal data to a legal order which does not ensure an adequate level of protection under of paragraph 2 of the preceding Article, provided that the controller ensures sufficient mechanisms to ensure the protection of privacy and the fundamental rights and freedoms of persons, as well as their performance, in particular by means of appropriate contractual clauses .

3. The transfer of personal data constituting the necessary measure for the protection of the defense, public security, prevention, investigation and prosecution of criminal offenses and the protection of public health shall be governed by specific legal provisions or by instruments of law interregional agreements to which São Tomé and Príncipe is bound.

Chapter VI
Notification and authorization

Article 21
Obligation to notify

1. The controller or his representative, if any, shall notify the National Agency for the Protection of Personal Data of the beginning of the performance in writing within eight days before the start of the treatment of a treatment or set of treatments, wholly or partly automated, for the pursuit of one or more interrelated purposes.

2. The National Agency for the Protection of Personal Data may authorize the simplification or exemption of notification for certain categories of processing which, in the light of the data to be processed, are not such as to jeopardize the rights and freedoms of data subjects and meet criteria of speed, economy and efficiency.

3. The authorization shall be published in the Diary of the Republic and shall specify the purposes of the treatment, the data or categories of data to be processed, the category or categories of data subjects, the recipients or categories of recipients to whom the data and the period of its conservation can be communicated.

4. Treatment shall be exempted from notification for the sole purpose of keeping records which, under the terms of a law or administrative regulation, are intended to inform the public and may be consulted by the general public or by a person who can prove a legitimate interest.

5. Non-automated processing of personal data referred to in Article 7 (1) shall be subject to notification when treated under Article 7 (3) (a).

Article 22

Pre- established control

1. Except as provided in paragraph 2 of this article, they require authorization from the National Agency for the Protection of Personal Data:

a) The processing of personal data referred to in Article 7 (2);

b) The processing of personal data relating to credit and the solvency of its holders;

c) The interconnection of personal data provided for in Article 9;

d) The use of personal data for purpose that isn't determinate to the collection.

2. The treatments referred to in the preceding paragraph may be authorized by legal provision or regulatory provision of an organic nature, and in this case, the authorization of the National Agency for the Protection of Personal Data is not required.

Article 23

Content of requests for an opinion or authorization and notification

Requests for an opinion or authorization, as well as notifications, sent to the National Agency for the Protection of Personal Data must contain the following information:

a) The name and address of the person responsible for the treatment and, where applicable, his representative;

b) The purposes of treatment;

c) A description of the category (s) of data holder and data or categories of personal data concerning them;

d) The recipients or categories of recipients to whom the data may be communicated and under what conditions;

e) Entity in charge of the processing of the information if it is not the person in charge of the treatment itself;

f) Possible interconnections of processing of personal data;

g) Time of retention of personal data;

h) The form and conditions that the holders of the data may have knowledge or correct the personal data concerning them;

i) Planned data transfers to other countries or territories;

j) A general description enabling a preliminary assessment of the adequacy of the measures taken to ensure the safety of the treatment in application of Articles 15 and 16.

Article 24
Mandatory indications

The legal provisions or regulatory provisions of an organic nature referred to in Article 7 (2) and Article 8 (1), as well as the authorizations of the National Agency for the Protection of Personal Data and records of personal data processing shall indicate at least:

a) The person responsible for the file or its representative;

b) The categories of personal data processed;

c) The purposes for which the data are intended and the categories of entities to whom it may be transmitted;

d) The manner of exercising the right of access and rectification;

e) Possible interconnections of processing of personal data;

f) Planned data transfers to other countries or territories.

2. Any change to the particulars referred to in paragraph 1 shall be subject to the procedures laid down in Articles 21 and 22.

Article 25
Advertising of treatments

1. The processing of personal data, when not subject to a legal or regulatory provision of an organic nature and must be authorized or notified, is registered with the National Agency for the Protection of Personal Data, open for consultation by any person.

2. The register shall contain the information listed in Article 23 (a) to (d) and (i).

3. The data controller not subject to notification is obliged to provide, at the least, the information referred to in paragraph 1 of the previous article, to any person requesting it.

4. The provisions of this Article shall not apply to proceedings the sole purpose of which is to maintain records which, under the terms of the law or administrative regulation, are intended to inform the public and are open for consultation by the general public or by any person prove a legitimate interest.

5. The National Agency for the Protection of personal data shall publish in its annual report all opinions and authorizations drawn up or granted under this Law, in particular the authorizations provided for in Articles 7 (2) and Article 9 (1).

Chapter VII
Codes of conduct

Article 26
Codes of conduct

1. The National Agency for the Protection of Personal Data encourages and supports the development of codes of conduct designed to contribute, according to the characteristics of the different sectors, to the proper implementation of the provisions of this Law and, in

general, to the self-regulation and in the realization and defense of fundamental rights related to the protection of privacy.

2. Professional associations and other organizations representing categories of data controllers who have drawn up draft codes of conduct may, if they so wish, submit them to the National Agency for the Protection of Personal Data for the purpose of registration.

3. If the National Agency for the Protection of Personal Data considers that the projects comply with the legal and regulatory provisions in force regarding personal data protection, it shall register them.

4. The registration of codes of conduct has an effect of mere declaration of legal compliance and these codes are not legal or regulatory norms.

Chapter VIII
Administrative and judicial protection

Section I
Administrative and judicial protection

Article 27
General Principle

Without prejudice to the right to submit complaints to the National Agency for the Protection of Personal Data, any person may, under the law, use administrative or judicial means to ensure compliance with legal and regulatory provisions on the protection of personal data

Article 28
Judicial protection

1. A decision rendered by a court shall always be subject to appeal to the Court of last instance on grounds of violation of the fundamental rights guaranteed by this Law, and the direct appeal and per shall be restricted to the question of breach and shall be of an urgent nature.

2. Without prejudice to the provisions of the preceding paragraph, an administrative court may resort to administrative acts or simply de facto de facto public channels, based on the violation of fundamental rights guaranteed in this Law, which is an urgent matter.

3. The provisions of the Code of Civil Procedure and the Code of Administrative Proceeding, respectively, shall apply to the procedural process of the judicial remedies provided for in the preceding paragraphs, with appropriate adaptations.

Section II
Administrative offenses

Article 29
Subsidiary legislation

The general system of administrative infringements, subject to the adaptations set out in the following Articles, shall be subject to the offenses provided for in this Section.

Article 30
Compliance with omitted duty

Where the administrative offense results from omission of a duty, the application of the penalty and the payment of the fine does not relieve the infringer of its compliance, if this can be possible.

Article 31
Omission or defective fulfillment of obligations

1. Entities that negligently failed to comply with the obligation to notify the National Agency for the Protection of Personal Data of the processing of personal data referred to in Article 21 (1) and (5), provide false information or comply with the notification obligation in breach of the terms set out in Article 23, or when, after being notified by the National Agency for the Protection of Personal Data, they maintain access to the open data transmission networks responsible for processing personal data that do not comply with the provisions of this Law, are guilty of an administrative offense punishable by the following fines:

a) In the case of a natural person, a minimum of 50,000,000.00 (fifty million Dobras) and a maximum of 120,000,000.00 (One Hundred and Twenty Million Dobras);

b) In the case of a group of persons without legal personality, a minimum of 100,000,000.00 (one hundred million Dobras) and a maximum of 200,000,000.00 (two hundred million Dobras);

c) In the case of a legal person, a minimum of 250,000,000.00 (two hundred and fifty million Dobras) and a maximum of 500,000,000.00 (five hundred million Dobras).

2. The fine shall be increased to double its thresholds in the case of data subject to prior checking in accordance with Article 22.

3. The criteria for applying the fines referred to in this article are regulated by the National Agency for the Protection of Personal Data.

Article 32
Other administrative offenses

1. Execute an administrative offense punishable by a fine of 25,000,000.00 (twenty five million Dobras) to 50,000,000.00 (fifty million Dobras), entities that do not comply with any of the following provisions of this Law established in Articles 5, 10, 11, 12, 13, 16, 17 and 25 (3).

2. When the obligations set forth in articles 6, 7, 8, 9, 19 and 20 are not complied with, the responsible entities commit an administrative offense is punishable by a fine of 45,000,000,00 (forty-five million Dobras) to 90,000,000.00 (ninety million Dobras).

Article 33
Competition of infringements

1. If the same event is both a crime and an administrative offense, the perpetrator shall always be punished as a criminal offense.

2. The penalties imposed on administrative offenses in competition shall always be materially cumulated.

Article 34
Punishment of negligence and attempted

1. Negligence shall always be punished in the administrative offenses referred to in Article 31.

2. The attempt shall always be punishable in respect of the administrative offenses referred to in the Articles 32 and 33.

Article 35
Application of fines

1. The application of the fines provided for in this Law is the responsibility of the National Agency for the Protection of Personal Data.

2. The decision of the National Agency for the Protection of personal data shall be enforceable if it is not challenged within the legal terms.

Section III
Crimes

Article 36
Non-compliance with data protection obligations

1. It is punishable by imprisonment up to one year or a fine of up to 120 days that intentionally:

a) Omit the notification or request for authorization referred to in Articles 21 and 22;

b) Provide false information in the notification or in the requests for authorization for the processing of personal data or in this procedure to make modifications not consented to by the instrument of legalization;

c) Divert or use personal data, in a manner incompatible with the purpose of the collection or with the instrument of legalization;

d) Promote or carry out an illegal interconnection of personal data;

e) Once the period established by the National Agency for the Protection of Personal Data has been exceeded in order to comply with the obligations provided for in this Law or in other data protection legislation,

f) After being notified by the National Agency for the Protection of Personal Data not to do so, maintain the access to open data transmission networks to those responsible for the processing of personal data that do not comply with the provisions of this Law.

2. The penalty shall be increased to double its thresholds in the case of personal data referred to in Articles 7 and 8.

Article 37
Bad access

1. Whoever, without any authorization, access to personal data whose access is forbidden, shall be punished with a prison sentence of up to one year or a fine of up to 120 days, if a penalty is more severe if the case does not fit for reasons of the special law.
The penalty shall be increased to double its limit when the access:

a) It is achieved through violation of technical safety rules;

b) Has allowed the agent or third parties the knowledge of personal data;

c) You have provided the agent or third parties, benefit or equity advantage.

3. In the case of paragraph 1, the criminal procedure depends on the complaint.

Article 38
Adding or destroying personal data

1. Who, without proper authorization, eliminate, destroy, damage, suppress or modify personal data, rendering them unusable or affecting their ability to use, shall be punished by imprisonment for up to two years or a fine of up to 150 days, if the penalty is more serious if the case does not fit by virtue of a special law.

2. The penalty shall be increased to double in its limits if the damage produced is particularly serious.

3. If the agent acts with negligence, the penalty is, in both cases provided for in the previous numbers, of imprisonment up to one year or a fine up to 120 days.

Article 39
Qualified disobedience

1. Whoever, after being notified for this purpose, does not interrupt, cease or block the processing of personal data, shall be punished with the penalty corresponding to the crime of qualified disobedience.

2. In the same sentence, who, after being notified:

a) To refuse, without just cause, the collaboration specifically requested by the National Agency for the Protection of Personal Data;

b) Not proceed with the elimination, total or partial destruction of personal data;

c)Do not destroy personal data at the end of the storage period provided for in Article 5.

Article 40
Breach of the duty of secrecy

1. Anyone who is bound by professional secrecy, without due cause and without due consent, reveals or discloses in whole or in part personal data, shall be punished by imprisonment for up to two years or a fine up to 150 days, if more serious penalty to the case does not fit by virtue of special law.

2. The penalty shall be increased by half of its limits if the agent:

a) For civil servant or equivalent, under the terms of the criminal law;

b) Is determined by the intention to obtain any patrimonial advantage or other illegitimate benefit;

c) Jeopardize the reputation, honor and consideration or privacy of another’s privacy.

3. Negligence shall be punishable by up to six months imprisonment or a fine of up to 120 days.

4. Outside the cases provided for in paragraph 2, the criminal procedure depends on the complaint.

Article 41
Try punishment

In the offenses provided for in this section, the attempt is always punishable.

Section IV
Accessory feathers

Article 42
Accessory penalty

In conjunction with the fines and penalties imposed on the sections II and III of this chapter, it may, in ancillary manner, be ordered:

a) a temporary or permanent ban on the processing, blocking, deletion or destruction of all or part of the data;

b) Publication of the conviction;

c) the public warning or censorship of the person responsible for processing by the National Agency for the protection of personal data.

Article 43
Publication of conviction

1. The condemnation shall be advertised in a periodical publication of great expansion in the Portuguese language, as well as by posting an edict in adequate format, for a period of not less than 30 days.

2. The publication shall be made by an extract containing the particulars of the infringement and the penalties applied, as well as the identification of the agent.

Chapter IX
Complementary provisions

Article 44
National Agency for the Protection of Personal Data

1. The following are approved by law of the National Assembly:

a) The organic law and the personalNAPPD;

b) The regime of incompatibility, impediment, suspension and loss of mandate, as well as the remuneration status of the members of the NAPPD.

2. The status of the members of the NAPPD guarantees the independence of the exercise of their functions.

3. NAPPD has its own framework for technical and administrative support.

Chapter X
Final and transitional provisions

Article 45
Transitional provision

1. Data processing in manual files at the date of entry into force of this Law shall comply with the provisions of Articles 7, 8, 10 and 11 within a period of 2 years.

2. In any case, the data holder may, at his request, and in particular when exercising his right of access, obtain, incomplete, inaccurate or irreparably stored, rectification, deletion or blocking of data for the legitimate purposes pursued by the controller.

3. The National Agency for the Protection of Personal Data may authorize that data contained in manual files and kept for historical research purposes only need not comply with Articles 7, 8 and 9, provided that it does not be re-used for a different purpose.

Article 46
Doubts and omissions

The doubts and omissions resulting from the interpretation and application of this Law are resolved in accordance with the general principles of law.

Article 47
Implementation

This Law shall enter into force in accordance with the law.

National Assembly, in São Tomé, on February 15, 2016.- The President of the National Assembly, José da Graça Diogo.

18th March 2016.

To be published.-

The President of the Republic, Manuel do Espírito SantoPinto da Costa
DIARY of the Republic