DATA PROTECTION ACT – THE REPUBLIC OF CAPE VERDE

LAW 133/V/2001 OF 22 JANUARY

This law establishes the general legal framework on the protection of individuals with regard to the processing of personal data.

CHAPTER I

General provisions

Article 1

Object

The present law establishes the general legal framework on the protection of individuals with regard to the processing of personal data.

Article 2

(Scope)

1. The present Act/Law shall apply to the processing of personal data wholly or partly by automated means as well as to the processing of personal data other than by automated means contained in manual files or part of manual files.
2. The present Act/Law shall apply to the processing of personal data carried out:
   a) in the context of the activities of an establishment of the controller situated within the national territory;
   b) outside the national territory in places where the Cape Verdean law applies by virtues of international public law;
   c) by a controller who is not established on the national territory, who for purposes of processing personal data makes use of automated or other types of equipment situated on the national territory except such equipment is used only for purposes of transit.
3. The present Act/Law shall apply to video surveillance and other forms of capture, processing and dissemination of sound and images permitting persons to be identified provided the processing controller is domiciled or based on the national territory or makes use of a computer or data communication network access provider established on the national territory.
4. In circumstances referred to subsection c) of number 2, the controller must designate by means of notification to the *Comissão Nacional de Protecção de Dados* (National Commission of Data Protection in English), henceforth referred to as CNPD (in Portuguese; NCDP in English), a representative established in Cape Verde to replace him in all his rights and obligations without prejudice to his own liability/responsibility.
5. The preceding number shall apply where the controller is covered by the status of extraterritoriality, immunity or any other status which precludes criminal proceedings.
6. This Act/Law shall to the processing of personal data regarding public safety, national defence and State security without prejudice to special rules in

instruments of international law to which Cape Verde is bound and specific laws pertinent to the respective sectors.

Article 3

(Exception to the scope)

The present Act/Law shall not apply to the processing of personal data carried out by individuals in the course of purely personal or household activities.

Article 4

(General principles)

The processing of personal data shall be carried out transparently and in strict respect for privacy and for other fundamental rights, freedoms and guarantees of the citizen.

Article 5

(Definitions)

For the purpose of this Act/Law:

a) "Personal data": shall mean any information of any type/nature and irrespective of the medium involved, including sound and image relating to an identified or identifiable person, "data subject";
b) "Processing of personal data" or " Processing" shall mean any operation or a set of operations which is performed upon personal data, whether wholly or partly, with or without automated means, such as collection, recording, organisation, storage, adaptation, or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment, or combination, as well as blocking, erasure or destruction;
c) "Personal data filing system" or "Filing system" shall mean any structured set of personal data which are accessible according to determined criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;
d) "Controller" shall mean the person or group, public authority, the service or any other entity/body that alone or jointly with others determine(s) the purposes or the means for the processing of personal data;
e) "Processor" shall mean a person or group, a public authority, agency or any other entity/body that processes personal data on behalf of the controller;
f) "Third party" shall mean a person or group, a public authority, agency or any other entity/body other than the data subject, the controller, the processor and the persons who under the direct authority of the controller or the processor, are authorised to process the data;
g) "Recipient" shall mean a person or group, a public authority, agency or any other entity/body to whom personal data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of the law shall not be regarded as recipients;

h) "The data subject's consent" shall mean any freely given specific and informed indication of his wishes by which the data subject gives his consent to his personal data being processed;
i) "Combination of data" shall mean a form of processing which consists of the possibility of correlating data in a filing system or systems kept by another or other controllers or kept by the same controller for other purposes.

2. In circumstances referred to in 1 a), a person is considered identifiable a person who may be directly or indirectly identified by means of an identification number or by means of one or more specific elements of his physical, physiological, psychological, economic, cultural or social characteristics.

3. In circumstances referred to in 1 d), whenever the purposes or processing means are determined by legislative provisions or regulations, the controller of the processing must be indicated in the law of the organisation and operations or in the statutes of the legal entity or statutorily competent for processing the personal data in question.

CHAPTER II

Processing of personal data

Section I

Data quality and lawfulness of their processing

Article 6

Data quality

1. Personal data must be:
   a) processed lawfully and with respect for the principle of good faith;
   b) collected for specific, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;
   c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
   d) accurate and, where necessary, kept up to date and adequate measures must be taken to ensure that data which are inaccurate or incomplete are erased or rectified having regard to the purposes for which they were collected or for which they are further processed;
   e) to be kept in a form that permits identification of their subjects for no longer than is necessary for the purposes for which they were collected or for which they are further processed.
2. Further processing of data for historical, statistical or scientific purposes as well as their being stored for the same purposes for a period longer than that referred to 1 e) above may be authorised by the CNPD at the request of the controller in instances of legitimate interest for long as it does compromise the rights, freedoms and guarantees of the data subject.
3. It shall be the responsibility of the controller to ensure that the above numbers are complied with.

Article 7

Criteria for making data processing legitimate

Personal data may be processed only if the data subject has unambiguously given his consent or if processing is necessary:

a) for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject;
b) for compliance with a legal obligation to which the controller is subject;
c) protection of vital interests of the data subject if the latter is physically or legally incapable of giving his consent;
d) for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed;
e) for pursuing the legitimate interests of the controller or the third party to whom the data are disclosed, except where such interests should be overridden by the interests or the fundamental rights, freedoms and guarantees of the data subject.

Article 8

The processing of sensitive data

1. The processing of personal data revealing philosophical, ideological or political beliefs or penalty, religion, political party or trade union affiliation, racial or ethnic origin, privacy, health and sex life, including genetic data shall be prohibited, except:

a) if the data subject expressed consent with the guarantee of non-discrimination and with adequate measure of assurance;
b) with foreseen legal authorisation with the guarantee of non-discrimination and with the adequate measure of assurance;
c) when the purpose of data processing are purely statistical, not individually identifiable with the adequate measure of assurance.

2. In granting authorisation foreseen in 1 b) the law must take into consideration particularly the indispensability of processing personal data referred to in 1 for performing legal attributions or statutory authorities for reasons of important public interest.
3. The processing of data referred to in 1 is also permitted when one of the following conditions applies:
    a) when it 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) when it is carried out with the data subject’s consent in the course of its legitimate activities by a foundation, association or non-profit seeking 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 it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects;

c) when it relates to data which are manifestly made public by the data subject, provided his consent for their processing can be clearly inferred from his declaration;
d) when it is necessary for the establishment, exercise or defence of legal claims and is exclusively carried out for that purpose.

4. The processing of personal data relating to health and sex life, including genetic data, shall be permitted if it is necessary for the purposes of preventive medicine, medical diagnosis, the provision of medical care or treatment or the management of health-care services, provided the processing of those data are done by a health professional bound by professional secrecy or by another person equally subjected to an equivalent professional secrecy and are notified to CNPD under article 23, and adequate information safety measures are guaranteed/provided.
5. The processing of data referred to in 1 may still be effected with adequate information security measures, when the indispensable security of the state, of public security, and the prevention, investigation or repression of penal infringements are demonstrated.

Article 9

(Suspicion of illegal activities, penalties, security measures, infringements, criminal and administrative offences)

1. Central registers relating to persons suspected of illegal activities, criminal and administrative offences and decisions applying penalties, security measures, fines and additional penalties may only be created and kept by public services vested with the specific responsibility by virtue of the law establishing their organisation and functioning, subject to observance of procedural and data protection rules provided for in a legal order, with the prior opinion of the of CNPD.
2. The processing of data related to persons suspected of illegal activities, criminal and administrative offences and decisions applying penalties, security measures, fines and additional penalties may be authorised by the CNPD, subject to observance of the rules for the protection of data and the security of information, when such processing is necessary for pursuing the legitimate purposes of the controller, provided the fundamental rights and freedoms of the data subject are not overridden.
3. The processing of personal data for the purposes of police investigations shall be restricted to the processing necessary to prevent a specific danger or to prosecute a particular offence and to exercise the responsibilities provided for in the respective implementing statutes or another legal provision or in the terms of international agreement or convention to which Cape Verde is a party.

Article 10

Combination of personal data

1. The combination of personal data not provided for in a legal provision shall be subject to the authorisation of the Parliamentary Committee of Investigation,

requested by the controller or jointly by the corresponding controllers under Article 23.

2. The combination of personal data must be necessary for pursuing the legal or statutory purposes and legitimate interests of the controller, must not involve discrimination or a reduction in the fundamental rights and freedoms of the data subjects, and must be covered by adequate security measures and take account of the type of data subject combination.

Section II

Rights of the data subject

Article 11

(Right to information)

1. The controller or his representative shall provide a data subject from whom data relating to himself are collected with the following information, except where he already has such information:
   a) the identity of the controller and of his representative, if any;
   b) the purposes of the processing;
   c) the recipients or categories of recipients;
   d) the obligatory or voluntary nature of the replies as well as the possible consequences of failure to reply;
   e) the existence and conditions of the right of access and the right to rectify provided they are necessary, considering specific circumstances of collection of the data in order to guarantee the data subject that they will be processed fairly;
   f) the decision of providing personal data for the first time to a third party for purposes provided in 13 c), previously and with expressed indication that it is his right to be against such communication;
   g) the decision that his personal data be used by a third party, previously and with expressed indication that it is his right to be against such communication;
2. The documents supporting the collection of personal data shall contain the information set down in the previous number.
3. If the data are not collected from the data subject and except where he already has such data, the controller or his representative must provide the data subject with the information set down in 1 at the time of undertaking the recording/registering of data or, if a disclosure to third parties is envisaged, no later than the time the data are first disclosed.
4. If data are collected from open networks, the data subject shall be informed, except where he is already aware of this, that personal data relating to him may be circulated on the network without security measures and may be at risk of being seen and used by unauthorised third parties.
5. The obligation to provide information may be waived for reasons of State security, crime prevention and investigation and also when processing data for statistical, historical and scientific research purposes, when the information/identification of the data subject would seem impossible involve a

disproportionate effort or when the law expressly determines the recording/registering of such data or its dissemination.

6. The obligation to provide information shall not apply to the processing of data carried out solely for journalistic purposes or the purpose of artistic or literary expression, except at the detriment of rights, freedoms and guarantees of the data subject.

Article 12

Right of access

1. The data subject has the right to obtain from the controller, without constraints, with reasonable intervals and without excessive delay or expense:
   a) confirmation as to whether or not data relating to him are being processed and information as to the purposes of the processing, the categories of data concerned and the recipients or categories of recipients to whom the data are disclosed;
   b) communication in an intelligible form of the data undergoing processing and of any available information as to their source;
   c) knowledge of the logic involved in any automatic processing of data concerning him, the automated decisions referred to as in 1 of Article 14;
   d) the rectification, erasure or blocking of data the processing of which does not comply with the provisions of the present law, especially due to the incomplete or inaccurate character of the data;
   e) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with d) unless this proves impossible or implies disproportionate effort.
2. In cases provided in 4 and 5 of Article 8, the right to access is exercised by means of the CNPD.
3. In the case provided in 6 of Article 11, the right of access is exercised by means of the CNPD, securing the constitutional rules applicable, in particular those guaranteeing freedom of expression and information, freedom of the press and the professional independence and secrecy of journalists.
4. In cases provided for in 2 and 3 of this Article, if communication of the data might jeopardise State security, the prevention and investigation of crime, and freedom of expression and information or freedom of the press, the CNPD shall only inform the data subject of the measures taken.
5. The right of access to information relating to health data, including genetic data, is exercised by means of the doctor chosen by the data subject.
6. If the data are used for taking measures or decisions regarding any particular individual(s), the law may restrict the right to access where there is clearly no risk of breaching the fundamental rights, freedoms and guarantees of the data subject, particularly the right to privacy, and when that data are used solely for purposes of scientific research or are kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics.

Article 13

(Data subject's right to object)

The data subject has the right to:

a) except where otherwise provided by law, and at least in cases referred to in Article 7 d) and e) to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, and where there is a justified objection, the processing effected by the controller may no longer involve those data;
b) to object on request and free of charge to the processing of personal relating to him which the controller anticipates being processed for the purposes of direct marketing or any other form of research, or to be informed before personal data are disclosed for the first time to third parties for the purposes of direct marketing or for use on behalf of third parties, and to be expressly offered the right to object free of charge to such disclosure or uses;
c) to object, without expense, that his personal data be communicated for the first time to third parties for purposes provided for in b) above or to be used by third parties.

Article 14

(Non-subjection to automated individual decisions)

1. Every person shall have the right not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, in particular his performance at work, creditworthiness, reliability or conduct.
2. Without prejudice to compliance with other provisions of this Law, a person may be subject to a decision taken under 1 if that decision is taken in the course of the entering into or performance of a contract, provided that the request for the entering into or the performance of the contract has been satisfied, or that there are suitable measures to safeguard his legitimate interests, particularly, arrangements allowing him to put his point of view.
3. The taking of a decision under 1 may also be permitted when authorised by the CNPD, which shall lay down measures to safeguard the data subject's legitimate interest.

Section III

Security and confidentiality of (data) processing

Article 15

(Security of processing)

1. The controller must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular when the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

2. The measures provided for in 1 above must ensure, considering the state of the art and the cost of their implementation, such measures shall ensure an adequate level of security appropriate to the risks represented by the processing face and the nature of the data to be protected.
3. When processing is carried out on his behalf, the controller must choose a processor providing sufficient guarantees in respect of the technical security measures and organisational measures governing the processing to be carried out, and must ensure compliance with those measures.
4. The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that the processor shall act only on instructions from the controller and that the obligations referred to in 1 shall also be incumbent on the processor.
5. Proof of the will to negotiate, the contract or the legal act relating to data protection and the requirements relating to the measures referred to in 1 shall be in writing in a supporting document legally certified as affording proof.

Article 16

(Special security measures)

1. The controllers of the data referred to in paragraphs of 1, in 2 and 5 of Article 8 and in 1 of Article 9 shall take adequate measures and added information security, particularly to:
   a) prevent unauthorised persons access to the premises used for processing data (control of entry to the premises);
   b) prevent data media from being read, copied, altered/modified by unauthorised persons (control of data media);
   c) prevent unauthorised input as well as unauthorised obtaining of knowledge, the alteration or elimination of personal data input (control of input);
   d) prevent automatic data processing systems from being used by unauthorised persons by means of data transmission premises (control of use);
   e) guarantee that authorised persons may only access data covered by authorisation (control of access);
   f) guarantee the checking of entities to whom personal data may be transmitted by means of data transmission premises (control of transmission);
   g) guarantee that it is possible to check *a posteriori*, in a period appropriate to the nature of the processing, the establishment in the regulations applicable to each sector of which personal data are introduced, when and by whom (control of input);
   h) prevent unauthorised reading, copying, altering, or eliminating of data in transmitting and transporting personal data (control of transport).
2. Taking account of the nature of the entities responsible for processing and the type of premises in which it is carried out, the CNPD may waive the existence of certain security measures, subject to guaranteeing respect for the fundamental rights, freedoms and guarantees of the data subjects.
3. The systems must guarantee the logical separation between data relating to health and sex life, including genetic data, and other personal data.

4. Where circulation over a network of the data referred to in 8 and 9 may jeopardise the fundamental rights, freedoms and guarantees of their data subjects, the CNPD may determine that transmission must be encoded.

Article 17

(Processing confidentiality)

Any person acting under the authority of the controller or the processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law.

Article 18

(Professional secrecy)

1. Controllers and persons who obtain knowledge of the personal data processed in carrying out their functions shall be bound by professional secrecy, even after their functions have ended.
2. Members of the CNPD shall be subject to the same obligation even after their mandate has ended.
3. The provision in the previous numbers shall not exclude the duty to supply the obligatory information according to the law, except when it is contained in filing systems organised for statistical purposes.
4. Officers/agents or staff who serve as consultants for the CNPD or its members are subjected to the same obligation of professional secrecy.

CHAPTER III

Transfer of personal data

SECTION I

Article 19

(Principles)

1. Without prejudice to the following Article, the transfer of personal data which are undergoing processing or intended for processing may only take place subject to compliance with the present Law and other legislation applicable to issues of personal data protection and, undergoing processing for transfer to another State, a country which has an adequate level of data protection.
2. The adequacy of the level of protection shall be assessed in light of all the circumstances surrounding a data transfer or set of data transfers, in particular, the nature of the data, the purpose and duration of the proposed processing, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the State in question, as well as the professional rules and security measures which are complied with in that country.
3. It is for the CNPD to decide whether a foreign State ensures an adequate level of protection.

Article 20

(Derogations)

1. The transfer of personal data to a State which does not ensure an adequate level of protection within the context of 19 2) may be allowed by the CNPD if the data subject has given his unequivocal consent to the proposed transfer or if that transfer:
   a) is necessary for the performance of a contract between the data subject and the controller of the processing the data or the precontractual measures taken in response to the request of the subject;
   b) is necessary for the execution/performance or the signing of a concluded or to be concluded contract in the interest of the data's subject between the controller and a third party;
   c) is necessary or legally required on the grounds of important public interest, or for the establishment, exercise of defence of legal claims;
   d) is necessary for the protection of vital interests of the data's subject;
   e) is made from a public register, within the contexts of the laws or regulations, is intended for information of the public and which is open to consultation either by the general public or by any person who can demonstrate legitimate interest provided the conditions laid down in law for consultation are fulfilled in this case.
2. Without prejudice to paragraph 1, the CNPD may authorise a transfer or set of transfers of personal data to a State which does not ensure an adequate level of protection within the meaning of Article 19 2) for as long as the processing controller provides adequate guarantees with respect to the protection of the privacy and fundamental rights and freedoms of individuals and with respect to their exercise, particularly by means of appropriate contractual clauses.
3. The transfer of personal data which is necessary for the protection of State security, defence, public safety and the prevention, investigation and repression of punishable criminal offences shall be governed by special legal provisions or by the international conventions to which Cape Verde is party.

CHAPTER IV

National authority for the investigation of the protection of personal data

Section I

General provisions

Article 21

(Objectives of the investigation)

The supervisory of personal data protection shall seek to follow-up, evaluate and control the activities of legally competent organs or services for its processing, safeguarding the fulfilment of the Constitution and the Law, especially the fundamental rights, freedoms and guarantees of citizens.

Article 22

(Nature of the investigation)

1. The supervisory of personal data protection is an independent administrative authority, CNPD, which operates within the National Assembly.
2. The CNPD is regulated by the Law.

Section II

Notification

Article 23

(Obligation to notify the CNPD)

1. The controller or his representative, if any, must notify the CNPD before carrying out any whole or partial automatic processing operation or set of operations intended to serve a single purpose or several purpose or several related purposes.
2. The CNPD may authorise the simplification of or exemption from notification for particular categories of processing which are unlikely, taking account of the data to be processed, to affect adversely the rights and freedoms of the data subjects and in to take account of criteria of speed, economy and efficiency.
3. The authorisation, which must specify the purposes of the processing, the data or categories of data to be processed, the category or categories of recipients to whom the data may be disclosed and the length of time the data are to be stored.
4. Processing whose sole purpose is the keeping of a register which according to law or regulations is intended to provide information to the public and which is open to consultation by the public in general or by nay person demonstrating a legitimate interest shall be exempted from notification.
5. The non-authorised processing of the personal data provided for in paragraph 1 of Article 8 shall be subject to notification when they are processed under Article 3 a).

Article 24

(Prior checking)

1. Except authorised by legal ruling, authorisation of the CNPD is required for:
   a) the processing of personal data referred to in subsections a) and e) of paragraph 1 of Article 8 and paragraphs 2 and 3 of Article 9;
   b) the processing of personal data relating to credit and the solvency of the data subjects;
   c) the combination of personal data as provided for in Article 9;
   d) the use of personal data for purposes not giving rise to their collection.
2. The legal ruling which authorises the processing of data referred to in the previous number requires the opinion of the CNPD.

Article 25

(Content of applications for opinions or authorisation and notification)

Applications for opinions or authorisations as well as notifications submitted to the CNPD shall include the following information:

a) the name and address of the controller and of his representative, if any;
b) the purposes of the processing;
c) the description of the category or categories of data subjects and of the data or categories of personal data relating to them;
d) the recipients or categories of recipients to whom the data might be disclosed and in what circumstances;
e) the entity entrusted with processing the information, if it is not the controller himself;
f) any combinations of personal data processing;
g) the length of time required for keeping personal data;
h) the form and circumstances in which the data subjects may be informed of or may correct the personal data relating to them;
i) proposed transfers of data to third countries;
j) a general description enabling a preliminary assessment to be made of the adequacy of the measures taken under Articles 15 and 16 to ensure security of processing.

Article 26

(Obligatory information)

1. The legal provisions referred to in subsection b) of paragraph 1 of Article 8 and paragraph 1 of Article 9 as well as the authorisation of the CNPD and the personal data processing filing system must, at least, indicate:
   a) the controller of the file and his representative, if any;
   b) the category of personal data processed;
   c) the purpose(s) of the data and the categories of the entities to whom they might be disclosed;
   d) the form of exercising the right of access and rectification;
   e) the combinations of personal data processing;
   f) the proposed transfers of data to third parties.
2. Any change in the information referred to in 1 shall be subject to the procedures provided in in Articles 23 and 24.

Article 27

(Publishing processing operations)

1. When personal data processing is not covered by a legal provision and must be authorised or notified it shall be set down in a CNPD register open to consultation by any person.
2. The register shall contain the information listed in paragraphs a) to d) and i) of Article 25.
3. The controller not subject to notification shall make available adequate information to any person that requests, at least, the information referred to in paragraph 1 of Article 26.
4. This Article does not apply to processing whose sole purpose is the keeping of a register which according to laws or regulations is intended to provide

information to the public and which is open to consultation either by the public in general or by any person who can provide proof of a legitimate interest.

5. The CNPD must indicate in its annual report all the opinions and authorisations drawn up and granted, particularly authorisations provided for in paragraph 1 of Article 8 and paragraph 2 of Article 10.

CHAPTER V

Codes of conduct

Article 28

Purposes

The codes of conduct are intended to contribute in relation to the characteristics of the different sectors for the proper implementation of the provisions of the present Law.

Article 29

Interventions of CNPD

1. The CNPD shall help in the elaboration of the codes of conduct.
2. Trade Associations and other entities representing other categories of controllers of data processing which have drawn up draft codes of conduct shall submit them for the appreciation of the CNPD.
3. The CNPD may declare whether the drafts are in accordance with the laws and regulations in force in the area of personal data protection.

CHAPTER VI

Legal/Judicial recourse, Liability, infringements and penalties

Section I

Legal/Judicial recourse and liability

Article 30

(Legal/Judicial recourse)

Without prejudice to the right to submit a complaint to the CNPD, according to the law any individual may seek legal recourse regarding violations of his rights granted him by the present law.

Article 31

(Liability)

1. Any person who has suffered damage as a result of an unlawful processing operation or any other act incompatible with legal provisions in the rea of personal data protection is entitled to receive compensation from the controller for the damage suffered.
2. The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the fact that give rise to the damage.

Section II

Infringements and penalties

Subsection

Offences

Article 32

(Subsidiary legislation)

The offences provided for in this subsection subsidiarily applicable to the system of offences with constant adaptations of the following/subsequent articles.

Article 33

(Omission or inadequate compliance with obligations)

1. Entities which negligently fail to comply with the obligation to notify the CNPD of the processing of personal data referred to in in paragraphs 1 and 5 of Article 23, provide false information or comply with the obligation to notify with observing the terms provided in Article 25, or after being notified by the CNPD, continue to allow access to open data transmission networks to controllers who fail to comply with the provisions of the Law are committing an offence punishable with the following fines:
   a) In the case a single individual a minimum of CVE 50,000 and a maximum of CVE 500,000;
   b) In the case of a group of people or an entity without legal personality a minimum of CVE 300,000 and a maximum of CVE 3,000,000.
2. The fine shall be increased to double the maximum in the case of data subject to prior authorisation according to article 24.

Article 34

(Other offences)

1. Entities which fail to comply with any of the following provisions of this law are committing an offence punishable with a minimum of CVE 100,000 and a maximum of CVE 1,000,000:
   a) Appointment of a representative according to paragraph 4 of Article 2;
   b) Observance of the obligations in Articles 6, 11, 12, 13, 14, 16, 17 and paragraph 3 of Article 27.
2. The fine shall be increased to double the maximum in the case of failure to comply with Articles 7, 8, 9, 10, 19 and 20.

Article 35

(Concurrent offences)

1. If the same fact is simultaneously a crime and an offence the agent shall always be punishable by virtue of the crime.
2. The penalties applied to concurrent offences shall always be materially accumulated.

Article 36

(Punishment of negligence and attempt)

1. Negligence shall always be punished in relation to offences provided for in Article 34.
2. Any attempt to commit an offence provided for in Articles 33 and 34 shall always be liable to punishment.

Article 37

(Application of fines)

1. The president of the CNPD is responsible for the application of the fines provided for in this Law subject to prior deliberation by the Commission.
2. The deliberations of the CNPD shall be enforceable if it is not challenged within the statutory period.

Article 38

(Compliance with duty omitted)

Whenever the offence arises from omitting a duty, application of the penalty and payment of the fine do not release the perpetrator from compliance with that duty, if it is possible.

Article 39

(Distribution of proceeds collected)

The sums collected as a result of the application of fines shall be for the CNPD.

Subsection II

Crimes

Article 40

(Non-compliance with obligations relating to data protection)

1. It is punishable with imprisonment of up to one year or a fine of up to 120 days, anyone who intentionally:
   a) omits notifications or the application for authorisation referred to in Articles 23 and 24;
   b) provides false information in the notification or in applications for authorisation for the processing of personal data or makes alterations in the latter which are not permitted by the legalisation instrument;
   c) misappropriates or uses personal data in a form incompatible with the purpose of the collection or with the legalisation instrument;
   d) promotes or carries out an illegal combination of personal data;
   e) fails to comply with the obligations provided for in this Law or in other data protection legislation when the time limit fixed by the CNPD for complying with them has expired;

f) continues to allow access to open data transmission networks to controllers who fail to comply with the provisions of this Act after notification by the CNPD not to do so.

2. The penalty shall be increased to double the maximum in the case of the personal data referred to in Article 8 and 9.

Article 41

(Undue access)

1. Any person who without due authorisation gains access by any means to personal data prohibited to him shall be liable to up tone year imprisonment or a fine of up to 120 days.
2. The penalty shall be increased to double the maximum when access:
   a) is achieved by means of violating technical security rules;
   b) allows the agent or third parties to obtain knowledge of the personal data;
   c) provides the agent or third parties with a benefit or material advantage.
3. In the case of 1 criminal proceedings are dependent upon a complaint.

Article 42

(Invalidation or destruction of personal data)

1. Any person who without the authorisation erases, destroys, damages, deletes, or changes personal data, making them unusable or affecting their capacity for use, shall be liable to up to two years imprisonment or a fine of up to 240 days.
2. The penalty shall be increased to double the maximum if the damage caused is particularly serious.
3. If the agents acts with negligence the penalty in both cases shall be up to one year imprisonment or a fine of up to 120 days.

Article 43

(Qualified non-compliance)

1. Any person who after being notified to do so does not interrupt, cease or block the processing of personal data shall be subject to a penalty corresponding to the crime of qualified non-compliance.
2. The same penalty shall apply to any person who after being notified:
   a) without just cause refuses to provide the collaboration specifically required of him by the CNPD according to the law;
   b) does not erase or totally or partially destroy the personal data;
   c) does not destroy the personal after the period for keeping them provided for in Article 6 has elapsed.

Article 44

(Violation of the duty of secrecy)

1. Any person bound by professional secrecy according to the law who without just cause and without due consent reveals or discloses personal data, totally or in part, shall be liable to imprisonment from six months to up to three years or a

fine of eighty to two hundred days, if the maximum penalty is applied to him corresponding to the gravity of his crime should he not be dismissed from his position or function.

2. The penalty shall be increased by half if the agent:
   a) is a civil servant or equivalent, according to penal law;
   b) acts with the intention of obtaining a material advantage or other unlawful gain;
   c) adversely affects the reputation, honour and esteem or the privacy of another person.
3. A person guilty of negligence shall be liable to up to six months imprisonment or a fine of up to 120 days.
4. Other than the cases provided in 2, criminal proceedings are dependent on a complaint.

Article 45

(Punishment of attempt)

Any attempt to commit the crimes provided for in the above provisions shall always be liable to punishment.

Article 46

(Additional penalties)

1. The following may be ordered in addition to the fines and penalties applied:
   a) temporary or permanent prohibition of processing, blocking, erasure or total or partial destruction of data;
   b) publication of the judgement;
   c) public warning or censure of the controller of the processing.
2. The judgement shall be published at the expense of the person judged in the periodical with the largest circulation published in the area of the district where the infringement was committed, or in a periodical in the nearest district, and by means of affixing a notice for a period of no less than 30 days.
3. Publication shall be done by means of a summary containing information on the offense and the penalties applied and the identification of the agent.

CHAPTER VII

Final Provisions

Article 47

(Existing manual filing system)

1. The processing of data held in manual filing systems on the date of the entry into force of this Law shall be brought into conformity with Articles 8, 9, 11 and 12 within six months.
2. At his request the data subject may in any event, in particular when exercising the right of access, obtain the rectification, erasure or blocking of incomplete or inaccurate data or data kept in a manner incompatible with the legitimate purposes of the controller.

3. The CNPD may provide that the data held in manual filing systems and kept solely for the purposes of historical research need not be brought into conformity with Articles 8, 9 and 10 provided they are in no case reused for a different purpose.

Article 48

(Existing automated filing system)

The existing automated files on the date of the entry into force of this Law must rigorously accomplish what those files and adapt them within a period of six months.

Article 49

(Entry into force)

This Law comes into force thirty days following its publication.

Approved on 20 December 2000.

The President of the *Assembleia Nacional*, *António do Espírito Santo Fonseca.*

Enacted on 10 January 2001.

Hereby published.

The President of the Republic of Cape Verde, ANTÓNIO MANUEL MASCARENHAS GOMES MONTEIRO.

Counter-signed on 13 January 2001.

The President of the *Assembleia Nacional*, *António do Espírito Santo Fonseca.*