ASSEMBLEIA DA REPÚBLICA [PORTUGUESE PARLIAMENT]

Act 67/98
of 26 October

Act on the Protection of Personal Data

(transposing into the Portuguese legal system Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data).

Under article 161 (c), article 165 (1) (b) and (c) and article 166 (3) of the Constitution, the *Assembleia da República* hereby decrees the following, which shall have the force of a general Act of the Republic:

CHAPTER I

General provisions

Article 1

Object

This Act transposes into the internal legal system Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Article 2

General principle

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

Article 3

Definitions

For the purposes of this Act:

(a) “personal data” shall mean any information of any type, irrespective of the type of medium involved, including sound and image, relating to an identified or identifiable natural person (“data subject”); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an indication number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

(b) “processing of personal data” (“processing”) shall mean any operation or set of operations which is performed upon personal data, whether wholly or partly by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

(c) “personal data filing system” (“filing system”) shall mean any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

(d) “controller” shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by laws or regulations, the controller shall be designated in the Act

establishing the organisation and functioning or in the statutes of the legal or statutory body competent to process the personal data concerned;

(e) "processor" shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

(f) "third party" shall mean any natural or legal person, public authority, agency or any other 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 natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a 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 signifies his agreement to personal data relating to him being processed;

(i) "combination of data" shall mean a form of processing which consists of the possibility of correlating data in a filing system with data in a filing system or systems kept by another or other controllers or kept by the same controller for other purposes.

Article 4

Scope

1 – This Act shall apply to the processing of personal data wholly or partly by automatic means, and to the processing other than by automatic means of personal data which form part of manual filing systems or which are intended to form part of manual filing systems.

2 – This Act shall not apply to the processing of personal data carried out by a natural person in the course of a purely personal or household activity.

3 – This Act shall apply to the processing of personal data carried out:

(a) in the context of the activities of an establishment of the controller on Portuguese territory;

(b) outside national territory, but in a place where Portuguese law applies by virtue of international public law;

(c) by a controller who is not established on European Union territory and who for purposes of processing personal data makes use of equipment, automated or otherwise, situated on Portuguese territory, unless such equipment is used only for purposes of transit through the territory of the European Union.

4 – This Act shall apply to video surveillance and other forms of capture, processing and dissemination of sound and images allowing persons to be identified, provided the controller is domiciled or based in Portugal or makes use of a computer or data communication network access provider established on Portuguese territory.

5 – In the circumstances referred to in paragraph 3 (c), the controller must designate, by means of notification to the *Comissão Nacional de Protecção de Dados* (CNPD), a representative established in Portugal to replace him in all his rights and obligations, without prejudice to his own liability.

6 – The preceding number shall apply where the controller is covered by the status of extraterritoriality, immunity or any other status which precludes criminal proceedings.

7 – This Act shall apply 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 Portugal is bound and specific laws pertinent to the respective sectors.

CHAPTER II

Processing of personal data

SECTION I

Data quality and the lawfulness of their processing

Article 5

Data quality

1 – Personal data must be:

(a) processed lawfully and with respect for the principle of good faith;

(b) collected for specified, 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; adequate measures must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;

(e) kept in a form which 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 – The storing of data for historical, statistical or scientific purposes for longer periods than in (e) above may be authorised by the CNPD at the request of the controller in the case of a legitimate interest.

3 – It shall be for the controller to ensure that the above numbers are complied with.

Article 6

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 or contracts to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract or a declaration of his will to negotiate;

(b) for compliance with a legal obligation to which the controller is subject;

(c) in order to protect the vital interests of the data subject if the latter if 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 for fundamental rights, freedoms and guarantees of the data subject.

Article 7

The processing of sensitive data

1 – The processing of personal data revealing philosophical or political beliefs, political party or trade union membership, religion, privacy and racial or ethnic origin, and the processing of data concerning health or sex life, including genetic data, shall be prohibited.

2 – The processing of the data referred to in the previous number shall be permitted by a legal provision or by the authorisation of the CNPD when, on important public interest grounds, such processing is essential for exercising the legal or statutory rights of the controller or when the data subject has given his explicit consent for such processing, in both cases with guarantees of non-discrimination and with the security measures provided for in Article 15.

3 – The processing of the data referred to in 1 shall also be 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 declarations;

(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 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 care or treatment or the management of health-care services, provided those data are processed by a health professional bound by professional secrecy or by another person also subject to an equivalent obligation of secrecy and are notified to the CNPD under article 27, and where suitable safeguards are provided.

Article 8

Suspicion of illegal activities, 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 that 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 CNPD.

2 – The processing of personal data relating 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 overriding.

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 an international agreement or convention to which Portugal is party.

Article 9

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 CNPD, requested by the controller or jointly by the corresponding controllers under Article 27.

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 to combination.

SECTION II

Rights of the data subject

Article 10

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 it:

(a) the identity of the controller and of his representative, if any;

(b) the purposes of the processing;

(c) other information such as:

The recipients or categories of recipients;

Whether replies are obligatory or voluntary, as well as the possible consequences of failure to reply;

The existence and conditions of the right of access and the right to rectify, provided they are necessary, taking account of the specific circumstances of collection of the data in order to guarantee the data subject that they will be processed fairly.

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 it, the controller or his representative must provide the data subject with the information set down in 1 at the time of undertaking the recording 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 on open networks the data subject shall be informed, except where he is already aware of it, 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 by a legal provision or decision of the CNPD on the grounds of State security and criminal prevention or investigation and also in particular for processing for statistical purposes or for the purposes of historical or scientific research, when the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law.

6 – The obligation to provide information under this Article shall not apply to the processing of data carried out solely for journalistic purposes or the purpose of artistic or literary expression.

Article 11

Right of access

1 – The data subject has the right to obtain from the controller without constraint at 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;

(d) The rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Act, in particular because of the incomplete or inaccurate nature 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.

2 – In the case of the processing of personal data relating to State security and criminal prevention or investigation, the right of access may be exercised by means of the CNPD or another independent authority in whom the law vests verification of compliance with legislation on the protection of personal data.

3 – In the cases provided for in 6 above 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 the cases provided for in (2) and (3), if communication of the data might prejudice State security, criminal prevention or investigation and freedom of expression and information or the 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 not used for taking measures or decisions regarding any particular individual, the law may restrict the right of 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 the 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 12
Data subject's right to object
The data subject has the right:
(a) save where otherwise provided by law, and at least in the cases referred to in Article 6 (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 instigated by the controller may no longer involve those data;
(b) to object, on request and free of charge, to the processing of personal data 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.

Article 13
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 the other provisions of this Act, 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 interests.

SECTION III
Security and confidentiality of processing
Article 14
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 where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.
2 – Where 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.
3 – 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.
4 – 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 15

Special security measures

1 - The controllers of the data referred to in Articles 7 (2) and Article 8 shall take appropriate measures to:

a) prevent unauthorised persons from entering the premises used for processing such data (control of entry to the premises);

b) prevent data media from being read, copied, altered or removed by unauthorised persons (control of data media);

c) prevent unauthorised input and unauthorised obtaining of knowledge, 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 the authorisation (control of access);

f) guarantee the checking of the bodies 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 input, when and by whom (control of input);

h) in transmitting personal data and in transporting the respective media, prevent unauthorised reading, copying, alteration or elimination of data (control of transport).

2 – Taking account of the nature of the bodies 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 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 articles 7 and 8 may jeopardise the fundamental rights, freedoms and guarantees of their data subjects the CNPD may determine that transmission must be encoded.

Article 16

Processing by a processor

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 17

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 act as consultants for the CNPD or its members shall be subject to the same obligation of professional secrecy.

CHAPTER III

Transfer of personal data

SECTION I

Transfer of personal data in the European Union

Article 18

Principle
Without prejudice to the tax or customs decisions of the Community, personal data may move freely between Member States of the European Union.

SECTION II
Transfer of personal data outside the European Union
Article 19
Principles
1 - Without prejudice to the following Article, the transfer to a State which is not a member of the European Union of personal data which are undergoing processing or intended for processing may only take place subject to compliance with this Act and provided the State to which they are transferred ensures an adequate level of protection.
2 – The adequacy of the level of protection of a State which is not a member of the European Union shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the State in question and the professional rules and security measures which are complied with in that country.
3 – It is for the CNPD to decide whether a State which is not a member of the European Union ensures an adequate level of protection.
4 – By means of the Ministry of Foreign Affairs the CNPD shall inform the European Commission of cases where it considers that a State does not ensure an adequate level of protection.
5 – The transfer of personal data identical to those the European Commission has considered do not enjoy adequate protection in the State to which they are to be sent shall be prohibited.

Article 20
Derogations
1 - A transfer of personal data to a State which does not ensure an adequate level of protection within the meaning of Article 19 (2) may be allowed by the CNPD if the data subject has given his consent unambiguously to the proposed transfer or if that transfer:
(a) is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request;
(b) is necessary for the performance or conclusion of a contract concluded or to be concluded in the interests of the data subject between the controller and a third party; or
(c) is necessary or legally required on important public interest grounds, or for the establishment, exercise of defence of legal claims; or
(d) is necessary in order to protect the vital interests of the data subject; or
(e) is made from 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 demonstrate legitimate interest, provided the conditions laid down in law for consultation are fulfilled in the particular case.
2 – Without prejudice to paragraph 1 the CNPD may authorise a transfer or a 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), provided the controller adduces adequate safeguards 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 - By means of the Ministry of Foreign Affairs the CNPD shall inform the European Commission and the competent authorities of the other Member States of the European Union of the authorisations it grants under 2.
4 – The authorisations provided for in 2 shall be granted or derogated by the CNPD according to its own procedures and the decisions of the European Commission.

5 – Whenever there are specimen contractual clauses approved by the European Commission according to its own procedures, because they provide the adequate guarantees referred to in 2, the CNPD shall authorise the transfer of personal data made under such clauses.
6 – A transfer of personal data which is necessary for the protection of State security, defence, public safety and the prevention, investigation and prosecution of criminal offences shall be governed by special legal provisions or by the international conventions and agreements to which Portugal is party.

CHAPTER IV
Comissão Nacional de Protecção de Dados
[National Data Protection Commission]
SECTION I
Nature, duties and responsibilities
Article 21
Nature
1 – The CNPD is an independent body with powers of authority which operates within the *Assembleia da República* .
2 - Whatever the national law applicable to the processing in question, the CNPD shall exercise its authority throughout national territory.
3 – The CNPD may be requested to exercise its powers by a data protection supervisory authority of another Member State of the European Union or the Council of Europe.
4 – The CNPD shall cooperate with the data protection supervisory authorities of other States in disseminating national law and regulations in the area of personal data protection and in the defence and exercise of the rights of individuals resident abroad.

Article 22
Duties
1 – The CNPD is the national authority endowed with the power to supervise and monitor compliance with the laws and regulations in the area of personal data protection, with strict respect for human rights and the fundamental freedoms and guarantees enshrined in the Constitution and the law.
2 – The CNPD must be consulted on any legal provisions and on legal instruments in preparation in Community or international institutions relating to the processing of personal data.
3 - The CNPD shall be endowed with:
(a) investigative powers, and may have access to data undergoing processing and powers to collect all the information necessary for the performance of its supervisory duties;
(b) powers of authority, particularly those of ordering the blocking, erasure or destruction of data, or imposing a temporary or permanent ban on the processing of personal data, even if included in open data processing networks from servers situated on Portuguese territory;
(c) the power to deliver opinions before processing is carried out and to ensure their publication.
4 – In the event of repeated failure to comply with legal provisions relating to personal data the CNPD may warn or publicly censure the processor, and in accordance with its duties may raise the matter with the*Assembleia da República* , the Government or other bodies or authorities.
5 – The CNPD is authorised to engage in legal proceedings where the provisions in this Act have been violated and must report to the Public Prosecution Service any criminal offences it becomes aware of in exercising and arising out of its functions, and shall take the necessary and urgent precautionary measures to provide the evidence.

6 – The CNPD is represented at law by the Public Prosecution Service and is exempt from costs in the proceedings in which it is involved.

Article 23
Responsibilities

1 - The CNPD is responsible in particular for:

(a) issuing opinions on legal provisions and on legal instruments in preparation in Community or international institutions relating to the processing of personal data;

(b) authorising or recording, as applicable, the processing of personal data;

(c) authorising in exceptional cases the use of personal data for purposes not giving rise to their collection, with respect for the principles laid down in Article 5;

(d) authorising the combination of data processed automatically in the cases provided for in Article 9;

(e) authorising the transfer of personal data in the cases provided for in Article 20;

(f) establishing the time for keeping the personal data according to their purpose, issuing directives for particular sectors of activity;

(g) ensuring the right of access to information and the exercise of the right of rectification and updating;

(h) authorising the establishment of costs or frequency for exercising the right of access and establishing the maximum periods for compliance in each sector of activity with the obligations which are incumbent upon the controller by virtue of articles 11 to 13;

(i) acting on an application made by any person or by an association representing that person concerning the protection of his rights and freedoms in regard to the processing of personal data and informing them of the outcome;

(j) checking the lawfulness of data processing at the request of any person whenever such processing is subject to restricted access or information, and informing the person that a check has taken place;

(k) assessing the claims, complaints or applications of private individuals;

(l) waiving the security measures according to Article 15 (2), issuing directives for particular sectors of activity;

(m) ensuring representation in joint supervisory proceedings and in Community and international meetings of independent personal data protection supervisory bodies, and taking part in international meetings within the scope of its responsibilities, in particular exercising representation and monitoring functions under the Schengen and Europol systems according to the applicable provisions;

(n) deliberating on the application of fines;

(o) promoting the drawing up of codes of conduct and assessing them;

(p) promoting the disclosure and clarification of rights relating to the protection of data and periodically publicising its activity, in particular by means of the publication of an annual report;

(q) exercising other legally established responsibilities.

2 – In exercising its responsibilities to issue directives or assess codes of conduct the CNPD must promote consideration of the views of the associations defending the interests concerned.

3 – In exercising its functions the CNPD shall lay down obligatory decisions against which challenges or appeals may be lodged with the *Tribunal Central Administrativo* [Central Administrative Court].

4 – The CNPD may suggest to the *Assembleia de República* the measures deemed useful for pursuing its duties and exercising its responsibilities.

Article 24
Duty to cooperate

1 - The public and private bodies shall cooperate with the CNPD by providing it with all the information requested in carrying out its responsibilities.

2 – The duty to cooperate shall be ensured in particular when in order to exercise its functions in full the CNPD has to examine the computer system and personal data filing systems, and all documentation relating to the processing and transmission of personal data.
3 – The CNPD or its members and the staff delegated thereby have the right of access to the computer systems supporting the data processing and the documentation referred to in the previous number, within the scope of its duties and responsibilities.

SECTION II
Composition and functioning
Article 25
Composition and mandate
1 – The CNPD shall be composed of seven members of recognised integrity and merit, the chairman and two members being elected by the *Assembleia de República* by means of the d'Hondt highest average rule.
2 – The remaining members shall be:
(a) two magistrates with over 10 years' experience, one being a legal magistrate appointed by the *Conselho Superior da Magistratura* , and the other a Public Prosecution Service magistrate appointed by the*Conselho Superior do Ministério Público* ;
(b) two individuals of recognised competence appointed by the Government.
3 – The members of the CNPD shall have a five-year mandate which shall cease when the newly appointed members take office.
4 - The members of the CNPD shall be set down on the list published in the 1 st series of the *Diário da República* .
5 – The members of the CNPD shall take office before the President of the *Assembleia de República* in the 10 days following publication of the list referred to in the previous number.

Article 26
Functioning
1 – The following shall be approved by an Act of the *Assembleia de República* :
(a) the implementing Act and the staff of the CNPD;
(b) the system of conflicts of interest, disqualification, suspension and loss of mandate, and the remuneration of the members of the CNPD.
2 – The status of the members of the CNPD guarantees their independence in exercising their functions.
3 – The Commission has its own staff for technical and administrative support, the respective officials and agents enjoying the status and benefits of the staff of the *Assembleia de República* .

SECTION III
Notification
Article 27
Obligation to notify the CNPD
1 – The controller or his representative, if any, must notify the CNPD before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single 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 to take account of criteria of speed, economy and efficiency.

3 – The authorisation, which must be published in the *Diário da República* , must specify the purposes of the processing, the data or category of data to be processed, the category or categories of data subjects, the recipients 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 laws or regulations is intended to provide information to the public and which is open to consultation by the public in general or by any person demonstrating a legitimate interest shall be exempted from notification.
5 – The non-automatic processing of the personal data provided for in Article 7 (1) shall be subject to notification when they are processed under 3 (a) of that Article.

Article 28
Prior checking
1 – The authorisation of the CNPD is required for:
(a) the processing of personal data referred to in Article 7 (2) and Article 8 (2);
(b) the processing of personal data relating to credit and the solvency of the data subjects;
(c) the combination of personal data provided for in Article 9;
(d) the use of personal data for purposes not giving rise to their collection.
2 – The processing referred to in the previous number may be authorised by legal ruling, in which case it does not require the authorisation of the CNPD.

Article 29
Content of applications for opinions or authorisation and notification
Applications for opinions, authorisation and 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) a 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 body entrusted with processing the information, if it is not the controller himself;
(f) any combinations of personal data processing;
(g) the length of time 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 14 and 15 to ensure security of processing.

Article 30
Obligatory information
1 – The legal provisions referred to in Article 7 (2) and Article 8 (1) and the authorisations of the CNPD and personal data filing systems must indicate at least:
(a) the controller of the file and his representative, if any;
(b) the categories of personal data processed;
(c) the purposes of the data and the categories of body to whom they might be disclosed;
(d) the form of exercising the right of access and rectification.;
(e) any combinations of personal data processing;
(f) proposed transfers of data to third countries.

2 – Any change in the information referred to in 1 shall be subject to the procedures provided for in Articles 27 and 28.

Article 31

Publicising of 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 Article 29 (a) to (d) and (i).

3 – A controller not subject to notification shall make available at least the information referred to in Article 30 (1) in an appropriate form to any person on request.

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 – All the opinions and authorisations drawn up or granted under this Act, particularly the authorisations provided for in Article 7 (2) and Article 9 (2), must be published by the CNPD in its annual report.

CHAPTER V

Codes of conduct

Article 32

Codes of conduct

1 – The CNPD shall encourage the drawing up of codes of conduct intended to contribute to the proper implementation of the provisions in this Act, taking account of the specific features of the various sectors.

2 – Trade associations and other bodies representing other categories of controllers which have drawn up draft codes of conduct shall be able to submit them to the opinion 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

Administrative and legal supervision

SECTION I

Administrative and legal supervision

Article 33

Administrative and legal supervision

Without prejudice to the right to submit a complaint to the CNPD, according to the law any individual may have recourse to administrative and legal means to guarantee compliance with legal provisions in the area of personal data protection.

Article 34

Liability

1 – Any person who has suffered damage as a result of an unlawful processing operation or of any other act incompatible with legal provisions in the area 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 event giving rise to the damage.

SECTION II

Administrative offences

Article 35
Subsidiary legislation
The general system of administrative offences, adapted according to the following articles, is subsidiarily applicable to the offences provided for in this section.

Article 36
Compliance with duty omitted
Whenever the administrative 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 still possible.

Article 37
Omission or inadequate compliance with obligations
1 – Bodies which negligently fail to comply with the obligation to notify the CNPD of the processing of personal data referred to in Article 27 (1) and (5), provide false information or comply with the obligation to notify without observing Article 29 or, having been notified by the CNPD, continue to allow access to open data transmission networks to controllers who fail to comply with the provisions of this Act are committing an administrative offence punishable with the following fines:
(a) In the case of a natural person, a minimum of PTE 50,000$00 and a maximum of PTE 500,000$00;
(b) In the case of a legal person or a body without legal personality, a minimum of PTE 300,000$00 and a maximum of PTE 3,000,000$00
2 – The fine shall be increased to double the maxima in the case of data subject to prior authorisation according to Article 28.

Article 38
Administrative offences
1 – Bodies which fail to comply with any of the following provisions of this Act are committing an administrative offence punishable with a minimum fine of PTE 100,000$00 and a maximum of PTE 1,000,000$00:
(a) Appointment of a representative according to Article 5 (4);
(b) Observance of the obligations in Articles 5, 10, 11, 12, 13, 15, 16 and 31 (3).
2 - The penalty shall be increased to double the maxima in the case of failure to comply with the obligations in Articles 6, 7, 8, 9, 19 and 20.

Article 39
Concurrent offences
1 - If the same fact is simultaneously a crime and an administrative offence the agent shall always be punished by virtue of the crime.
2 – The penalties applied to concurrent administrative offences shall always be materially accumulated.

Article 40
Punishment of negligence and attempt
1 – Negligence shall always be punished in relation to the administrative offences provided for in Article 38.
2 - Any attempt to commit the administrative offences provided for in Articles 37 and 38 shall always be liable to punishment.

Article 41
Application of fines
1 – The chairman of the CNPD is responsible for the application of the fines provided for in this Act, subject to prior deliberation by the Commission.

2 – After being approved by the chairman the deliberation of the CNPD shall be enforceable if it is not challenged within the statutory period.

Article 42
Distribution of proceeds collected
The sums collected as a result of the application of fines shall be divided equally between the State and the CNPD.

SECTION III
Crimes
Article 43
Non-compliance with obligations relating to data protection
1 –Any person who intentionally:
(a) omits notification or the application for authorisation referred to in Articles 27 and 28;
(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 Act 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,
shall be liable to up to one year's imprisonment or a fine of up to 120 days.
2 – The penalty shall be increased to double the maxima in the case of the personal data referred to in Articles 7 and 8.

Article 44
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 to one year's imprisonment or a fine of up to 120 days.
2 - The penalty shall be increased to double the maxima 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 45
Invalidation or destruction of personal data
1 – Any person who without due 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 maxima if the damage caused is particularly serious.

3 – If the agent acts with negligence the penalty in both cases shall be up to one year's imprisonment or a fine of up to 120 days.

Article 46
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 cooperation specifically required of him according to Article 24;
(b) does not erase or totally or partially destroy the personal data;
(c) does not destroy the personal data after the period for keeping them provided for in Article 5 has elapsed.

Article 47
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 up to two years' imprisonment or a fine of up to 240 days.
2 - The penalty shall be increased by half the maxima 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 for in 2, criminal proceedings are dependent upon a complaint.

Article 48
Punishment of attempt
Any attempt to commit the crimes provided for in the above provisions shall always be liable to punishment.

Article 49
Additional penalty
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, according to Article 22 (4).
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 otherwise 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 offence and the penalties applied and the identification of the agent.

CHAPTER VII
Final provisions
Article 50
Transitional provision
1 – The processing of data held in manual filing systems on the date of the entry into force of this Act shall be brought into conformity with Articles 7, 8, 10 and 11 within five years.

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 7, 8 and 9, provided they are in no case reused for a different purpose.

Article 51
Revocation
Acts 10/91 of 29 April and 28/94 of 29 August are hereby revoked.

Article 52
Entry into force
This Act comes into force on the day following its publication.

Approved on 28 September 1998.

The President of the *Assembleia da República* , *António de Almeida Santos* .

Enacted on 7 October 1998.

Hereby published.

The President of the Republic, JORGE SAMPAIO.

Counter-signed on 14 October 1998.

The Prime Minister, *António Manuel de Oliveira Guterres* .

https://www.cnpd.pt/english/bin/legislation/Law6798EN.HTM