



Strasbourg, 4 September 1991

20784
Restricted
CJ-PD (91) 33

COMMITTEE OF EXPERTS ON DATA PROTECTION
(CJ-PD)

Law for the protection of personal data
with regard to automatic processing

P O R T U G A L

Law 10/91
29 April 1991

By virtue of Articles 164 (d), 168 (1) (b), (c) and (d), and 169 (3) of the Constitution, the Assembly of the Republic hereby decrees as follows:

CHAPTER I

General provisions

Article 1

General principle

The processing of data shall be conducted transparently and with complete respect for private and family life and the citizen's rights, freedoms and fundamental guarantees.

Article 2

Definitions

For the purposes of this Law:

- a) "personal data" means any information relating to an identified individual or one who is identifiable in a way which does not involve disproportionate expenditure or time;
- b) "public data" means personal data included in public official documents, except such confidential items as profession and address and any disabilities shown on a birth certificate;
- c) "computer system" means one or more computers with peripheral equipment and software for the processing of data;
- d) "automated data file" means any structured set of data undergoing automatic processing whether centralized or scattered in different locations;
- e) "data base" means a set of interrelated data, stored and structured with redundancy check, intended for one or more forms of data processing;

- f) "data bank" means a set of data relating to or able to be related to a particular matter;
- g) "automatic processing" means the following operations if carried out in whole or in part by automated means: storage of data, carrying-out of logical and/or arithmetical operations on those data, and their alteration, erasure, retrieval or dissemination;
- h) "controller of the file" means the natural or legal person, public authority, agency or any other body which is competent to decide what should be the purpose of the automated data file, data bank or data base; which categories of personal data should be stored and which operations should be carried out on them;
- i) "transborder data flows" means the circulation of personal data across national frontiers.

Article 3

Scope

1. This Law shall apply to:
 - a) the setting-up and keeping of automated files, data bases and data banks containing personal data;
 - b) data media concerning legal persons and equivalent bodies, when exter these contain personal data.
2. This Law shall not apply to personal data files containing only information intended for:
 - a) personal or domestic use;
 - b) the processing of employees' wages and salaries, and other administrative procedures for day-to-day management;
 - c) invoicing for goods or services supplied;
 - d) the collection of membership subscriptions.
3. The Law shall also not apply to personal data files set up and kept under the responsibility of the Intelligence System of the Portuguese Republic.

CHAPTER II

The National Commission for the Protection of Automated Personal Data

Article 4

Constitution and purpose

1. A National Commission for the Protection of Automated Personal Data (CNPDPPI) shall be set up, in order to supervise the automatic processing of personal data, in strict compliance with human rights requirements and the freedoms and guarantees enshrined in the Constitution and in law.
2. The CNPDPI shall be an independent public authority, reporting to the Assembly of the Republic and possessing its own technical and administrative support services.

Article 5

Composition

1. The CNPDPI shall be composed of seven members of recognized integrity and merit, its chairman and two members being elected by the Assembly of the Republic, on the d'Hondt method of voting.
2. The other members shall be:
 - a) two legal officials with more than ten years' service, one a judge appointed by the Conselho Superior da Magistratura and the other a prosecutor appointed by the Conselho Superior do Ministério Público;

- b) two persons of recognized competence in the matter, appointed by the Government.

Article 6

Duties and incompatibilities

1. Members of the CNPDPI must be citizens enjoying their full civil and political rights.
2. As regards their duties and incompatibilities, members of the CNPDPI shall be governed by the same general principles as apply to officials and employees of the State.
3. Membership of the CNPDPI shall be incompatible with the holding of:
 - a) government office, including in the governments of the autonomous regions;
 - b) office in local government;
 - c) executive posts in political parties or special interest associations or any form of employment by them.

Article 7

Remuneration

The remuneration of members of the CNPDPI shall be determined by the Government.

Article 8

Tasks

1. The tasks of the CNPDPI shall be to:
 - a) issue opinions on the setting-up, altering or holding by public bodies automated data files, data banks and data bases

- containing personal data, as provided for in this Law;
- b) authorise or record, as the case may be, the setting-up, altering or holding by other bodies of automated data files, data banks and data bases containing personal data, in accordance with this Law;
 - c) authorise, in exceptional cases provided for in this Law and subject to strict control, the use of personal data for purposes other than those for which they were collected;
 - d) authorise, in exceptional cases provided for by this Law and subject to strict control, the interconnection of automated data files, data banks and data bases containing personal data;
 - e) issue guidelines for guaranteeing the security of data, both when stored and when being processed in telecommunications networks;
 - f) lay down general rules for access to data and exercise of the right to have data corrected and updated;
 - g) ensure that the appropriate judicial authorities take the decisions necessary to stop the processing of data, prevent the operation of files and, if necessary, have them destroyed, in the cases provided for in this Law;
 - h) assess claims, complaints or requests from individuals, as provided for in this Law;
 - i) publish an annual report on its activity;
 - j) report to the prosecuting authorities such infringements of this Law as require prosecutions.
2. In carrying out its duties, the CNPDPI shall issue binding decisions, appeals against which may be made to the Higher Administrative Court (Supremo Tribunal Administrativo).
3. The CNPDPI may propose to the Assembly of the Republic such measures as it considers appropriate for it to fulfil its purpose and carry out its tasks.

Article 9

Duty to cooperate

In carrying out its duties, the CNPDPI shall be entitled to the cooperation of all public and private bodies.

Article 10

Taking up office

1. The members of CNPDPI shall be sworn in before the President of the Assembly of the Republic, with ten days of publication of its membership in the Diario da Republica, first series.
2. The CNPDPI's period of office shall be five years, continuing until a new Commission is sworn in.
3. Upon coming into operation, the CNPDPI shall immediately draft its own rules of procedure, which shall be submitted for approval by the Assembly of the Republic.

CHAPTER III

Automatic processing of personal data

Article 11

Limitations on the processing of data

1. There shall be no automatic processing of personal data concerning:
 - a) philosophical or political convictions, membership of political parties or trade unions, religious belief or private life;
 - b) racial origin, criminal convictions, suspected illegal activity, health, property and wealth.

2. The prohibition set out in the previous paragraph shall not prevent processing of data for research or statistical purposes, provided the persons concerned are not identifiable.
3. Automatic processing of personal data as referred to in paragraph 1 (b) above may however be carried out by public bodies, in accordance with law, provided there is no discrimination and subject to the approval by the CNPDPI.
4. The preceding paragraphs shall not prevent automatic processing of personal data by an institution to which the data have been voluntarily supplied by the persons concerned, in full knowledge of the use to be made of them.

Article 12

Requirements for collection

1. Personal data for automatic processing shall be collected in a fair and lawful manner.
2. Personal data must be collected in a way which is appropriate to the purpose for which they are being collected.
3. The purpose for which data are collected must be known before collection begins.

Article 13

Right of information and access

1. Any person shall be entitled to be informed of the existence of an automated data file, data bank or data base containing personal data concerning him and of its purpose, as well as of the identity and address of its controller.
2. Access to files of electoral data shall be permitted, on a basis

of equality and under the control of the National Electoral Commission, to political parties and candidates.

Article 14

Updating of data

Personal data collected and held in automated data files, data banks and data bases must be accurate and up to date.

Article 15

Use of data

Except as authorized by law, personal data may be used only for the purpose for which they were collected.

Article 16

Restriction of legal judgment

No legal, administrative or disciplinary decision involving an assessment of human behaviour may be based only on or result from the automatic processing of information concerning the profile of personality of the data subject.

CHAPTER IV

Automated data files, data bases and data banks
containing personal data

Article 17

Requirements for setting up files

1. The setting-up of automated files, data bases and data banks containing personal data, for the purposes referred to in Article 11, must be authorized by law, after approval by the CNPDPI.
2. Paragraph 1 above shall not apply to automated data files, data banks and data bases held by public or private bodies and not containing personal data as referred to in Article 11.
3. The bodies referred to in the previous paragraph shall, however, be obliged to inform the CNPDPI in advance of the setting-up of automated files, data bases and data banks containing other personal data and shall communicate the particulars set out in the following Article.

Article 18

Procedure for requests

Requests for opinions or authorisation from the CNPDPI regarding setting-up or holding automated data files, data banks and data bases containing personal data, and communications as referred to in Article 17 (3), shall include the following particulars:

- a) The name and address of the controller of the file;
- b) the characteristics and purpose of the file;
- c) the body or bodies responsible for processing the data;
- d) the personal data contained in each individual file;
- e) the way in which data are to be collected and updated;

- f) the purpose of the data, the bodies to which they may be communicated and subject to what conditions;
- g) the comparisons, interconnections or any other kind of linking which may be established between the data stored;
- h) the measures taken to guarantee the security of data;
- i) the period during which personal data have to be kept;
- j) the category of persons having direct access to data;
- k) the way in which the data subject may be informed of the data concerning him, and subject to what conditions;
- l) the way in which the data subject may have any inaccuracies in data concerning him corrected.

Article 19

Mandatory particulars

1. Laws as referred to in Article 17 (1) and CNPDPI authorizations is referred to in Article 8 (1) (c) and (d) shall indicate:
 - a) the controller of the file;
 - b) the personal data to be held in each individual file;
 - c) the way in which data are to be collected or updated;
 - d) the purpose for which data are intended, the bodies to which they may be communicated and subject to what conditions;
 - e) the length of time personal data may be kept;
 - f) the way in which the data subject may be informed of data concerning him, and subject to what conditions;
 - g) the way in which the data subject may have any inaccuracies in data concerning him corrected.

2. Any alteration to the particulars referred to in paragraph 1 shall also be covered by a law and/or by CNPDPI authorization, depending on the case.

Article 20

Operation of files

1. Controllers of automated files, data banks and data bases containing personal data shall immediately stop their operation when, for acting in contravention of this Law, they receive instructions to that effect from the competent authority.
2. Without prejudice to any other penalties, automated files as referred to in the previous paragraph may be prevented from operating and, if necessary, their content destroyed.

Article 21

Security systems

Automated files, data banks and data bases containing personal data must be equipped with security systems which not only prevent them being consulted, altered, destroyed or added to by unauthorized persons but also enable any leaks of information, whether intentional or not, to be detected.

CHAPTER V

Collection and interconnection of personal data

Article 22

Indications in documents for collecting data

1. Documents used for collecting personal data shall indicate:
 - a) the fact that the data, or some of them, are to be automatically processed;
 - b) whether it is compulsory or optional to fill in the documents or supply the data;

- c) what are the consequences of no or wrong answers being given;
 - d) the persons for whom the data are intended;
 - e) the purpose of collecting data;
 - f) the controller of the file, with his address;
 - g) the conditions of access referred to in Article 27 and 28.
2. The preceding paragraph shall not apply to the collection of information for the prevention and punishment of crime or for statistical purposes, as provided for in the legislation on the National Statistical System and the National Statistics Institute.

Article 23

Destruction of data

After their authorized keeping time data must be destroyed, unless the period is extended by specific law or authorization by the CNPDPI, according to the case.

Article 24

Interconnection of personal data

1. The interconnection of automated files, data bases and data banks containing personal data is prohibited, except as provided for in this Law.
2. It is forbidden to allocate a single identification number in order to interconnect automated files of personal data containing information concerning police matters, criminal convictions or medical details.

Article 25

Interconnection of public data

Automated files, data bases and data banks containing only public data may be interconnected between bodies using them for the same specific purposes, if they have the same controller as referred to in Article 2 (h).

Article 26

Exceptional cases

Any law allowing, in exceptional case, the interconnection of automated files, data banks or data bases shall set out expressly the types of interconnection allowed and their purpose.

CHAPTER VI

Rights and guarantees of individuals

Article 27

Right of access to data

Without prejudice to the Law concerning State secrets and confidentiality in judicial proceedings, any individual, provided he is properly identified, shall be entitled to have access to data concerning him contained in automated files, data banks and data bases.

Article 28

Exercise of the right to access

1. The conditions for access to data shall not be such to restrict it, but may be subject to rules designed to prevent abuse.
2. Data shall be supplied in plain language, without any coded component, and shall strictly reflect the content of the file.
3. Medical data, however, shall be communicated to the person they concern through a doctor designated by that person.

Article 29

Excessive data and missing data

When an automated file, data bank or data base containing personal data is found to contain excessive amounts of such data for its designed purpose or has relevant data missing, the controller of the file shall immediately delete excessive data or incorporate omitted data.

Article 30

Incorrect data

1. Any person shall be entitled to have any incorrect data referring to him corrected, any data which are totally or partially missing added, and any information obtained by unfair or unlawful means, or whose recording or keeping are not permitted, deleted.
2. It shall be for the data subject to prove that the information is false if it was supplied by him or with his consent, or if he did not fulfil a legal obligation to communicate a change.

3. Any person shall be entitled to required his name and address to be deleted from files used for direct mailing.

Article 31

Action by the controller of the file

1. In the cases referred to in the two previous articles, the controller of the file shall comply with the wishes of the individual concerned or communicate with him to any other effect, within 30 days.
2. The data subject may submit a complaint to the CNPDPI concerning the actions of the controller of the file.

Article 32

Professional secrecy

1. Controllers of automated files, data banks and data bases and persons who, in the course of their work, become acquainted with the personal data recorded in them shall be subject to the obligation of professional secrecy.
2. Members of the CNPDPI shall also be subject to the same obligation, including after their term of office.
3. The above provisions shall not prejudice the obligation for information to be supplied in accordance with law, with the exception of files for statistical purposes.

CHAPTER VII

Transborder data flows

Article 33

1. The provisions of this Law shall apply to transborder flows, by whatever medium, of personal data undergoing automatic processing or collected with a view to their being automatically processed.
2. The CNPDPI may, however, authorize transborder data flows if the State of destination provides protection equivalent to that under this Law.
3. Transborder flows of personal data shall in any case be prohibited if there is good reason to believe that the aim of transfer to another State is to circumvent prohibitions or conditions laid down in this Law or to make it possible for the data to be used unlawfully.

CHAPTER VIII

Infringements and penalties

Article 34

Illegal use of data

1. Any person who, in infringement of the Law, sets up, maintains or modifies the content of an automated file, data bank or data base containing personal data or has such data processed, shall be liable to imprisonment for up to one year or to a fine of up to 120 days.

2. The penalty shall be doubled in the case of personal data as referred to in Article 11, where such processing is not authorised.
3. The same penalties shall apply, to any person intentionally using personal data for any purpose other than that laid down by law for their collection and use.

Article 35

Denial of access

1. Any person who by Law is obliged to guarantee another person's right of access to and to correct or add to personal data in an automated file, data bank or data base and refuses, without good reason, to do so or on purpose does so incorrectly or incompletely shall be liable to imprisonment for up to one year or a fine of up to 120 days.
2. If the person concerned acted negligently, he shall be liable to imprisonment for up to 3 months or a fine of up to 90 days.
3. Criminal proceedings shall depend upon a complaint being made.

Article 36

Illegal interconnection

1. Any person who, in infringement of this Law, effects or abets the interconnection of automated files, data banks or data bases containing personal data shall be liable to imprisonment for up to one year or to a fine of up to 120 days.
2. The penalty shall be doubled in the case of data as referred to in Article 11.

3. The preceding paragraphs shall apply to violation of the prohibition laid down in Article 24 (2).
4. The courts shall lay down such measures as are necessary for ending the interconnection of files, data banks or data bases and for deleting a number as referred to in Article 24 (2), if this has not been done by the time of judgment

Article 37

False information

1. Any person who supplies false information in the application for authorisation to set up or maintain an automated file, data bank or data base containing personal data or who carries out thereon modifications not provided for in the instrument of authorisation shall be liable to imprisonment for up to two years or a fine of up to 240 days.
2. The same penalty shall apply to any person intentionally omitting to make the communication referred to in Article 17 (3).
3. Is the person concerned acted negligently, he shall be liable to imprisonment for up to 6 months or a fine of up to 100 days.

Article 38

Improper access

1. Any person who, without appropriate authorisation, accesses in any way an information system containing personal data access to which is forbidden to him shall be liable to imprisonment for up to one year or a fine of up to 120 days.

2. The above penalties shall be doubled where such access:
 - a) was achieved by violating technical security rules;
 - b) enabled the person concerned or third parties to obtain knowledge of data;
 - c) procured for the person concerned or any third parties, with their knowledge, any profit or property advantage.
3. In the case referred to in paragraph 1, criminal proceedings shall depend upon a complaint being made.

Article 39

Damaging or destroying data

1. Any person who, without being duly authorised thereto, deletes, destroys, damages or alters, so as to render them unusable or less useable, personal data contained in an automated file, data bank or data base shall be liable to imprisonment for up to two years or a fine of up to 240 days.
2. The above penalties shall be doubled should the damage caused be particularly serious.
3. If the person concerned acted negligently, he shall be liable to imprisonment for up to 1 year or a fine of up to 120 days.

Article 40

Contempt of Court

1. Any person who, having been duly instructed to do so, fails to halt the operation of an automated file, data bank or data base containing personal data, in accordance with Article 20, shall be liable to the penalty for contempt of Court.
2. The same penalty shall apply to any person who:
 - a) refuses without just cause to collaborate under Article 9, when duly instructed to do so;

- b) does not destroy personal data after the time limit for keeping them referred to in Article 23.

Article 41

Violation of professional secrecy

1. Any person subject under law to professional secrecy who, without just cause and without due permissions, discloses all or some personal data contained in an automated file, data bank or data base, so jeopardizing the reputation, honour or privacy of any other person, shall be liable to imprisonment for up to two years or a fine of up to 240 days.
2. The above penalties shall be increased by one half if the person concerned:
 - a) is a public official or equivalent, within the meaning of the criminal law;
 - b) was motivated by the intention to obtain any property advantage or other unlawful benefit.
3. If the person concerned acted negligently, he shall be liable to imprisonment for up to six months or a fine of up to 120 days.
4. Except in the cases referred to in paragraph 2, criminal proceedings shall depend upon a complaint being made.

Article 42

Attempts to commit offences

Any attempt to commit the offences referred to above shall be punishable.

Article 43

Additional penalty

In addition to the main penalties imposed, the court may order the additional penalty of the conviction being published, in whole or in part, at the expense of the person convicted, in one or more periodical publications.

CHAPTER IX

Transitional and final provisions

Article 44

Organization

1. Persons in charge of public services maintaining automated files, data banks or data bases containing personal data shall draw up and submit through the appropriate channels, within six months, draft rules concerning them which will bring them into conformity with this Law.
2. Within one year the Government shall publish the necessary legal provisions for making the changes referred to in the previous paragraph.

Article 45

Existing files

1. Bodies as referred to in Article 12 (3) which are responsible for automated files, data banks or data bases containing personal data which are already in operation, shall, within 90 days of the

CNPDPI being set up, inform it of their existence and operation, as provided for in Article 18.

2. Authorisation to maintain files not yet authorised under this Law shall be requested from the CNPDPI within one year of its being set up.
3. Authorisation by the CNPDPI shall be granted within 60 days of the date of receipt of the application.
4. Failure to comply with paragraph 1 shall lead to application of Article 20 (2).

Approved on 19 February 1991

The President of the Assembly of the Republic,
Vitor Pereira Crespo

Promulgated on 9 April 1991

Let it be published.

The President of the Republic, Mário Soares

Counter signed on 12 April 1991

The Prime Minister, Aníbal António Cavaco Silva

