Organic Law 15/1999, of December 13, on the Protection of Personal Data.

JUAN CARLOS I

KING OF SPAIN

All those who were present saw and understood.

Know: That the Cortes Generales have approved and I come to sanction the following Organic Law.

TITLE I

General disposition

Article 1. Purpose.

The purpose of this Organic Law is to guarantee and protect, with respect to the processing of personal data, public freedoms and fundamental rights of natural persons, and especially their honor and personal and family privacy.

Article 2. Scope of application.

1. This Organic Law will apply to personal data recorded on physical media, making them susceptible to treatment, and any form of subsequent use of these data by the public and private sectors.

This Organic Law will govern all processing of personal data:

A) When the treatment is carried out in Spanish territory in the framework of the activities of an establishment of the person in charge of the treatment.

B) When the controller of treatment not established in Spanish territory, the Spanish law is applicable to the application of rules of public international law.

C) When the controller is not established in the territory of the European Union and uses in the processing of average data located in Spanish territory, unless such means are used only for transit purposes.

2. The regime for the protection of personal data established in this Organic Law will not apply:

A) Files kept by natural persons in the exercise of exclusively personal or domestic activities.

B) To files subject to the regulations on the protection of classified material.

C) Files established for the investigation of terrorism and serious forms of organized crime. However, in these cases, the person responsible for the file will first communicate the existence of the file, its general characteristics and its purpose to the Data Protection Agency.

3. The following processing of personal data will be governed by its specific provisions, and by the special provision, where appropriate, by this Organic Law:

A) The files regulated by the electoral regime legislation.

B) Those that serve exclusively statistical purposes, and are protected by the state or autonomous legislation on the public statistical function.

C) Those that have as object the storage of the data contained in the personal reports of qualification to which the legislation of the personnel regime of the Armed Forces refers.

D) The derivatives of the Civil Registry and the Central Registry of convicts and rebels.

E) Those from images and sounds obtained through the use of video cameras by the Security Forces and Bodies, in accordance with the legislation on the subject.

Article 3. Definitions.

For the purposes of this Organic Law, the following definitions shall apply:

A) Personal data: any information concerning identified or identifiable natural persons.

B) File: any organized set of personal data, whatever the form or modality of creation, storage, organization and access.

C) Data processing: operations and technical procedures of an automated nature or not, which allow the collection, recording, preservation, elaboration, modification, blocking and cancellation, as well as transfers of data resulting from communications, consultations, interconnections and transfers.

D) Responsible for the file or treatment: natural or legal person, public or private, or administrative body, deciding on the purpose, content and use of the treatment.

E) Affected person or interested party: natural person who holds the data that are subject to the treatment referred to in section c) of this article.

F) Dissociation procedure: any processing of personal data in such a way that the information obtained can not be associated with an identified or identifiable person.

G) Responsible for the treatment: the natural or legal person, public authority, service or any other body that, alone or jointly with others, treats personal data on behalf of the controller.

H) Consent of the interested party: any free, unambiguous, specific and informed expression of will, through which the interested party consents to the processing of personal data concerning him / her.

I) Transfer or communication of data: any disclosure of data made to a person other than the data subject.

J) Sources accessible to the public: those files whose consultation can be carried out by any person, not impeded by a limiting rule or without more exigency than, if appropriate, the payment of a consideration.

Only the promotional census, the telephone repertoires in the terms provided by its specific regulations and the lists of persons belonging to groups of professionals that contain only the data of name, title, profession, activity, Academic degree, direction and indication of their group membership. Public newspapers and newsletters and the media also have the character of public access sources.

TITLE II

Principles of data protection

Article 4. Quality of data.

1. Personal data may only be collected for processing and subjected to such processing, where appropriate, relevant and not excessive in relation to the specific, explicit and legitimate scope and purpose for which it was obtained.

2. Personal data subject to treatment may not be used for purposes incompatible with those for which the data had been collected. Subsequent processing of such data for historical, statistical or scientific purposes shall not be considered incompatible.

3. The personal data will be accurate and updated so that they respond truthfully to the current situation of the affected.

4. If the personal data recorded to be inaccurate, in whole or in part, or incomplete, will be canceled and replaced ex officio by the corresponding corrected or completed data, without prejudice to the faculties that the affected recognize article 16.

5. Personal data will be canceled when they are no longer necessary or relevant for the purpose for which they were collected or registered.

They shall not be kept in a form that allows the identification of the interested party for a period greater than that necessary for the purposes on which they were collected or registered.

Regulations shall determine the procedure by which, by exception, when historical, statistical or scientific values are taken into account in accordance with the specific legislation, the maintenance of certain data is decided in full.

6. Personal data will be stored in a way that allows the exercise of the right of access, unless legally canceled.

7. The collection of data by fraudulent, unfair or illegal means is prohibited.

Article 5. Right of information in the collection of data.

1. The interested parties to whom personal data are requested must be informed in advance in an express, precise and unequivocal manner:

A) The existence of a file or processing of personal data, the purpose of the collection of these and the recipients of the information.

B) The obligatory or optional nature of their response to the questions raised.

C) The consequences of obtaining the data or the refusal to supply them.

D) The possibility of exercising the rights of access, rectification, cancellation and opposition.

E) The identity and address of the controller or, where appropriate, his / her representative.

When the controller is not established in the territory of the European Union and uses in the processing of average data located in Spanish territory, he shall designate, unless such means are used for processing purposes, a representative in Spain, without prejudice to The actions that could be taken against the person in charge of the treatment.

2. When questionnaires or other forms are used for the collection, the warnings referred to in the previous section shall be clearly legible in the same.

3. The information referred to in paragraph 1 (b), (c) and (d) shall not be required if the content of the information is clearly inferred from the nature of the personal data requested or from the circumstances in which they are collected.

4. When the personal data has not been collected from the interested party, the data subject must be informed in an express, precise and unequivocal manner by the person responsible for the file or his representative within three months of the date of registration of the data, Unless previously informed, of the content of the processing, of the origin of the data, as well as of what is foreseen in paragraphs a), d) and e) of paragraph 1 of this article.

5. The provisions of the previous section, when expressly provided by law, when the treatment has historical, statistical or scientific purposes, or when the information to the interested party is impossible or requires disproportionate efforts, at the discretion of the Agency. Data Protection or equivalent autonomous body, taking into account the number of interested parties, the age of the data and the possible compensatory measures.

Likewise, the provisions of the previous section shall also not apply when the data come from sources accessible to the public and are used for advertising or commercial prospecting, in which case, in each communication addressed to the interested party, Data and the identity of the person responsible for the treatment as well as the rights that assist him / her.

Article 6. Consent of the affected.

1. The treatment of personal data will require the unequivocal consent of the affected person, unless otherwise provided by law.

2. Consent shall not be required when personal data are collected for the exercise of the functions of public administrations within the scope of their powers; When they refer to the parties to a contract or pre-contract of a business, labor or administrative relationship and are necessary for its maintenance or compliance; When the processing of the data is intended to protect a vital interest of the interested party in the terms of Article 7 (6) of this Law, or when the data appear in sources accessible to the public and their processing is necessary for the satisfaction of the interest Legitimate aim pursued by the person responsible for the file or by the third party to whom the data are communicated, provided that the fundamental rights and freedoms of the data subject are not violated.

3. The consent referred to in the article may be revoked where there is justified cause and no retroactive effect.

4. In cases where the consent of the data subject is not necessary for the processing of personal data, and provided that a law does not provide otherwise, the latter may oppose its treatment when there are well-founded and legitimate grounds relating to a Concrete personal situation. In such case, the person responsible for the file will exclude from the processing the data related to the affected.

Article 7. Particularly protected data.

1. According to what is established in section 2 of Article 16 of the Constitution, no one may be forced to testify about their ideology, religion or beliefs.

When, in relation to these data, the consent referred to in the following paragraph is sought, the interested party shall be advised of his right not to lend it.

2. Only personal data revealing ideology, trade union affiliation, religion and beliefs may be processed with the express written consent of the affected party. The files held by political parties, trade unions, churches, confessions or religious communities and associations, foundations and other non-profit organizations, whose purpose is political, philosophical, religious or trade union,

with respect to data relating to their associates, are excepted. Or members, without prejudice to the fact that the transfer of such data will always require the prior consent of the affected party.

3. Personal data that refer to racial origin, health and sexual life can only be collected, treated and transferred when, for reasons of general interest, a law or the affected person expressly consents.

4. Files created for the sole purpose of storing personal data revealing ideology, trade union affiliation, religion, beliefs, racial or ethnic origin, or sex life are prohibited.

5. Personal data relating to the commission of criminal or administrative offenses may only be included in files of the competent Public Administrations in the cases provided for in the respective regulatory standards.

6. Notwithstanding the provisions of the preceding paragraphs, the personal data referred to in paragraphs 2 and 3 of this article may be processed, where such treatment is necessary for the prevention or for the medical diagnosis, the benefit Health care or medical treatment or the management of health services, provided that such processing is carried out by a health professional subject to professional secrecy or by another person also subject to an equivalent obligation of secrecy.

The data referred to in the previous paragraph may also be processed when the treatment is necessary to safeguard the vital interest of the affected person or of another person, in the event that the affected person is physically or legally incapable of giving consent.

Article 8. Health information.

Without prejudice to what is provided in article 11 regarding the assignment, public and private institutions and health centers and the corresponding professionals may proceed to the treatment of personal data related to the health of the persons who come to them Or must be treated in them, in accordance with the provisions of state or autonomous legislation on health.

Article 9. Data security.

1. The person responsible for the file and, where appropriate, the person in charge of the processing shall adopt the necessary technical and organizational measures to guarantee the security of personal data and prevent its alteration, loss, treatment or unauthorized access, Taking into account the state of the technology, the nature of the data stored and the risks to which they are exposed, whether arising from human action or from the physical or natural environment.

2. Personal data shall not be recorded in files that do not meet the conditions established by regulation regarding their integrity and safety and those of treatment centers, premises, equipment, systems and programs.

3. Regulations shall establish the requirements and conditions to be met by the files and persons involved in the processing of the data referred to in article 7 of this Law.

Article 10. Duty of secrecy.

The person responsible for the file and those who intervene at any stage in the processing of personal data are bound to the professional secrecy with respect to them and to the duty to keep them, obligations that will subsist even after terminating their relationship with the owner of the file or, in Your case, with the person responsible for it.

Article 11. Communication of data.

1. Personal data subject to processing may only be communicated to a third party for the fulfillment of purposes directly related to the legitimate functions of the assignor and the assignee with the prior consent of the interested party.

2. The consent required in the previous section will not be precise:

A) When the assignment is authorized in a law.

B) In the case of data collected from sources accessible to the public.

C) When the treatment responds to the free and legitimate acceptance of a legal relationship whose development, compliance and control necessarily imply the connection of said treatment with third party files.

In this case the communication will only be legitimate as long as it is limited to the purpose that justifies it.

D) When the communication to be effected is addressed to the Ombudsman, the Public Prosecutor or the Judges or the Court of Auditors, in the exercise of the functions assigned to him. Neither consent will be required when the communication is addressed to autonomous institutions with functions similar to the Ombudsman or the Court of Auditors.

E) Where the assignment occurs between public administrations and has as its object the subsequent processing of the data for historical, statistical or scientific purposes.

F) When the transfer of personal data related to health is necessary to solve an emergency that requires access to a file or to carry out epidemiological studies in the terms established in the legislation on state or regional health.

3. The consent to the communication of personal data to a third party shall be null and void where the information provided to the interested party does not allow him to know the purpose for which the data for which the communication is authorized or the type of activity of that person to be used Who intend to communicate.

4. Consent to the communication of personal data is also revocable.

5. The one to whom the personal data are communicated is bound, by the mere fact of the communication, to the observance of the provisions of this Law.

6. If the communication is made after a decoupling procedure, the provisions of the previous sections will not be applicable.

Article 12. Access to data on behalf of third parties.

1. Data communication shall not be considered as the access of a third party to the data when such access is necessary for the provision of a service to the controller.

2. The performance of treatments on behalf of third parties must be regulated in a contract that must be in writing or in some other way that can prove their conclusion and content, expressly stating that the data controller will only treat the data according to the instructions of the Responsible for the treatment, which shall not apply or use them for a purpose other than that contained in said contract, nor communicate them, not even for their conservation, to other persons.

The contract shall also stipulate the security measures referred to in article 9 of this Law that the person in charge of the treatment is obliged to implement.

3. Once the contractual provision has been fulfilled, the personal data must be destroyed or returned to the controller, as well as any support or documents that contain any personal data that is the subject of the treatment.

4. In the event that the data controller assigns the data to another purpose, communicates them or uses them in breach of the terms of the contract, he will also be considered responsible for the processing, responding to the infractions that he personally incurred.

TITLE III

People rights

Article 13. Challenging valuations.

1. Citizens have the right not to be subjected to a decision with legal effects, on them or that affects them in a significant way, that is based only on a treatment of data intended to evaluate certain aspects of their personality.

2. The person affected may challenge administrative acts or private decisions that imply an assessment of their behavior, the only basis being a processing of personal data that offers a definition of their characteristics or personality.

3. In this case, the affected person shall have the right to obtain information from the person responsible for the file on the evaluation criteria and the program used in the treatment that served to adopt the decision in which the act consisted.

4. The assessment of the behavior of citizens, based on a data processing, can only have probative value at the request of the affected.

Article 14. Right to consult the General Registry of Data Protection.

Any person may know, seeking for this purpose the timely information from the General Data Protection Register, the existence of personal data processing, its purposes and the identity of the person responsible for the treatment. The General Registry shall be of public consultation and free of charge.

Article 15. Right of access.

1. The interested party shall have the right to request and obtain, free of charge, information on their personal data processed, the origin of said data, as well as the communications made or expected to be made.

2. The information may be obtained by simply consulting the data through its visualization, or indicating the data that are processed by means of a written, copy, fax or photocopy, certified or not, in a legible and intelligible form, without Use codes or codes that require the use of specific mechanical devices.

3. The right of access referred to in this article may only be exercised at intervals of not less than twelve months, unless the interested party establishes a legitimate interest to that effect, in which case they may exercise it earlier.

Article 16. Right of rectification and cancellation.

1. The controller shall have the obligation to enforce the right of rectification or cancellation of the interested party within a period of ten days.

2. Personal data whose processing does not comply with the provisions of this Law and, in particular, where such data are inaccurate or incomplete, will be rectified or canceled.

3. The cancellation will result in the blocking of the data, being only available to the Public Administrations, Judges and Tribunals, for the attention of the possible responsibilities born of the treatment, during the period of prescription of these.

Once that period has expired, the deletion must be carried out.

4. If the rectified or canceled data has been previously communicated, the controller must notify the rectification or cancellation made to the person who has communicated, in the case that the processing by the latter is maintained, that it must also proceed with the cancellation .

5. Personal data shall be kept during the periods provided for in the applicable provisions or, as the case may be, in the contractual relations between the person or entity responsible for the treatment and the interested party.

Article 17. Opposition, access, rectification or cancellation procedure.

1. The procedures for exercising the right of opposition, access, as well as the right of rectification and cancellation shall be established by regulation.

2. No consideration shall be required for the exercise of the rights of opposition, access, rectification or cancellation.

Article 18. Protection of rights.

1. The actions that are contrary to the provisions of this Law may be subject to a complaint by the interested parties before the Data Protection Agency, in the form that is determined by regulation.

2. The person to whom the exercise of opposition, access, rectification or cancellation rights is denied, in whole or in part, may inform the Data Protection Agency or, where appropriate, the competent body of each Community Autónoma, which must ensure the provenance or unlawfulness of the denial.

3. The maximum term in which the express resolution of protection of rights must be given will be of six months.

4. The decisions of the Data Protection Agency shall be subject to judicial review.

Article 19. Right to compensation.

1. The interested parties who, as a result of the breach of the provisions of this Law by the person responsible for the treatment, suffer damage or injury in their property or rights shall be entitled to compensation.

2. In the case of publicly owned files, liability shall be required in accordance with the legislation governing the liability regime of public administrations.

3. In the case of files of private ownership, the action will be exercised before the bodies of ordinary jurisdiction.

TITLE IV

Sectoral provisions

CHAPTER I

Publicly-owned files

Article 20. Creation, modification or deletion.

1. The creation, modification or deletion of the files of the Public Administrations may only be made by means of a general provision published in the Official State Gazette or corresponding Official Gazette.

2. Provisions for the creation or modification of files shall indicate:

A) The purpose of the file and the intended uses for it.

B) The persons or groups on which it is intended to obtain personal data or that are obliged to supply them.

C) The procedure for the collection of personal data.

D) The basic structure of the file and the description of the types of personal data included in it.

(E) Transfers of personal data and, where appropriate, transfers of data to third countries.

F) The bodies of the Administrations responsible for the file.

G) The services or units to which the rights of access, rectification, cancellation and opposition can be exercised.

H) Security measures with indication of the basic level, medium or high demandable.

3. In the provisions that are dictated for the deletion of the files, the destination of the files or, if appropriate, the forecasts that are adopted for their destruction will be established.

Article 21. Communication of data between public administrations.

1. The personal data collected or elaborated by the Public Administrations for the performance of their attributions will not be communicated to other Public Administrations for the exercise of different competences or of competences that deal in different subjects, except when the communication had been foreseen by The provisions for creating the file or by a higher-level provision regulating its use, or where the communication is for the purpose of further processing of the data for historical, statistical or scientific purposes.

2. In any case, personal data that a public administration obtains or elaborates for another may be subject to communication.

3. Notwithstanding what is established in article 11.2.b), the communication of data collected from sources accessible to the public may not be made to files of private ownership, but with the consent of the interested party or when a law provides otherwise.

4. In the cases provided for in paragraphs 1 and 2 of this article, the consent of the person referred to in article 11 of this Law shall not be necessary.

Article 22. Files of the Security Forces and Bodies.

1. Files created by the Forces and Security Corps containing personal data that, because they have been collected for administrative purposes, must be subject to permanent registration, will be subject to the general regime of this Law.

2. The collection and processing of personal data by the security forces without the consent of the persons concerned are limited to those assumptions and categories of data that are necessary for the prevention of a real danger to public safety Or for the repression of criminal offenses, and must be stored in specific files established for this purpose, which must be classified by categories according to their degree of reliability.

3. The collection and treatment by the Security Forces of the data referred to in Article 7 (2) and (3) may be carried out exclusively in cases where it is absolutely necessary for the purposes of a specific investigation, without Prejudice to the control of legality of the administrative action or of the obligation to resolve the claims made in the case by the interested parties that correspond to the courts.

4. Personal data recorded for police purposes will be canceled when they are not necessary for the inquiries that led to their storage.

For this purpose, the age of the person concerned and the nature of the data stored, the need to maintain the data until the conclusion of a specific investigation or procedure, the final judicial decision, in particular acquittal, pardon, rehabilitation And the prescription of responsibility.

Article 23. Exceptions to rights of access, rectification and cancellation.

1. Those responsible for the files containing the data referred to in paragraphs 2, 3 and 4 of the previous article may deny access, rectification or cancellation depending on the dangers that may arise for the defense of the State or security Public, the protection of the rights and freedoms of third parties or the needs of the investigations being carried out.

2. Those responsible for the files of the Public Treasury may also refuse to exercise the rights referred to in the previous paragraph when it obstructs administrative actions aimed at ensuring compliance with tax obligations and, in any case, When the affected person is subject to inspections.

3. The affected party, who is totally or partially denied the exercise of the rights mentioned in the previous sections, may inform the Director of the Data Protection Agency or the competent body of each Autonomous Community in the case of files kept By their own Police Bodies, or by the Autonomous Tax Administrations, who must ensure the provenance or inadmissibility of the denial.

Article 24. Other exceptions to the rights of those affected.

1. The provisions of paragraphs 1 and 2 of article 5 shall not apply to the collection of data when the information to the affected person seriously impedes or hinders compliance with the control and verification functions of public administrations or when it affects National Defense , Public safety or the prosecution of criminal or administrative offenses.

2. The provisions of article 15 and paragraph 1 of article 16 will not be applicable if, when weighted the interests in presence, the rights given by said precepts to the affected would have to yield to reasons of public interest or interests of Third parties more worthy of protection. If the administrative body responsible for the file invokes the provisions of this section, it shall issue a reasoned decision and instruct the person affected by the right that assists him to notify the Director of the Data Protection Agency or, where appropriate, the equivalent body Of the Autonomous Communities.

CHAPTER II

Privately owned files

Article 25. Creation.

Private files may be created that contain personal data when it is necessary for the achievement of the legitimate activity or object of the person, company or entity and respect the guarantees established by this Law for the protection of individuals.

Article 26. Notification and registration.

1. Any person or entity that creates files of personal data will notify the Data Protection Agency in advance.

2. By means of regulations, a detailed regulation of the different extremes of the notification shall be made, including the person responsible for the file, the purpose of the file, its location, the type of personal data it contains, Security measures, indicating the basic, medium or high level required and the transfers of personal data that are expected to be carried out and, where appropriate, the transfer of data that are foreseen to third countries.

3. Changes to the purpose of the automated file, its manager and the address of its location must be communicated to the Data Protection Agency.

4. The General Registry of Data Protection will register the file if the notification complies with the requirements.

Otherwise, you may request that the missing data be completed or corrected.

5. After one month from the submission of the application for registration without the Data Protection Agency has resolved on it, it will be understood that the automated file is registered for all purposes.

Article 27. Communication of the transfer of data.

1. The person in charge of the file, at the time of the first assignment of data, must inform those affected, indicating also the purpose of the file, the nature of the data that have been assigned and the name and Address of the assignee.

2. The obligation established in the previous section shall not exist in the case provided for in Article 11 (2) (c), (d), (e) and (6), or when the assignment is required by law.

Article 28. Data included in sources of public access.

1. The personal data contained in the promotional census, or lists of persons belonging to groups of professionals referred to in article 3, j) of this Law shall be limited to those that are strictly necessary to fulfill the purpose Intended for each listing. The inclusion of additional data by the entities responsible for the maintenance of such sources will require the consent of the interested party, which may be revoked at any time.

2. The interested parties shall be entitled to have the entity responsible for the maintenance of the listings of professional associations indicate freely that their personal data can not be used for advertising or commercial prospecting purposes.

The interested parties will have the right to demand free of charge the exclusion of all of their personal data that are included in the promotional census by the entities in charge of the maintenance of said sources.

The attention to the request to exclude unnecessary information or to include the objection to the use of the data for purposes of advertising or distance selling must be made within ten days in respect of information that is made through consultation or telematic communication And in the next edition of the list whatever the medium in which it is edited.

3. Public access sources that are published in the form of a book or some other physical medium, will lose the character of accessible source with the new edition that is published.

In the event that a copy of the list is electronically obtained in electronic form, it will lose the character of public access within a period of one year, counted from the moment of its obtaining.

4. Data contained in publicly available telecommunication service guides shall be governed by specific regulations.

Article 29. Provision of information services on solvency and credit.

1. Those engaged in the provision of information services on solvency and credit may only process personal data obtained from records and sources accessible to the public established for this purpose or from information provided by the data subject or his feelingly.

2. Personal data relating to the fulfillment or non-fulfillment of monetary obligations provided by the creditor or by the person acting on his behalf or interest may also be processed. In these cases, the interested parties will be notified in respect of those who have registered personal data in files, within thirty days from that registration, a reference of those that have been included and will be informed of their right to collect information from All of them, in the terms established by this Law.

3. In the cases referred to in the two preceding paragraphs, when the interested party so requests, the controller will communicate the data, as well as the evaluations and assessments that have been communicated during the last six months and the name And address of the person or entity to whom the data have been disclosed.

4. Only personal data that are decisive for the economic solvency of the interested parties and which do not refer, when adverse, to more than six years, can be recorded and transferred, provided that they respond truthfully to the current situation of those.

Article 30. Treatments for advertising and commercial prospecting purposes.

1. Those engaged in the collection of addresses, document distribution, advertising, distance selling, commercial prospecting and other similar activities shall use names and addresses or other personal data when they appear in sources accessible to the public or when Been provided by the parties concerned or obtained with their consent.

2. When the data come from sources accessible to the public, in accordance with what is established in the second paragraph of article 5.5 of this Law, each communication addressed to the interested party will inform the origin of the data and the identity of the person responsible for the Treatment, as well as the rights that assist him.

3. In the exercise of the right of access, the interested parties shall have the right to know the origin of their personal data, as well as the other information referred to in article 15.

4. The interested parties will have the right to oppose, on request and without expenses, the processing of the data concerning them, in which case they will be removed from the treatment, canceling the information contained therein at their simple request.

Article 31. Promotional census.

1. Those who intend to carry out permanently or sporadically the activity of collecting addresses, document distribution, advertising, distance selling, commercial prospecting or other similar activities may request from the National Statistical Institute or from the equivalent bodies of the Autonomous Communities a copy Of the promotional census, formed with the data of name, surnames and address that are recorded in the electoral census.

2. The use of each promotional census list will have a term of validity of one year. After the deadline, the list will lose its character as a source of public access.

3. The procedures by which the interested parties may request not to appear in the promotional census will be regulated by regulations. Among these procedures, which will be free for those interested, will include the registration document.

An updated list of the promotional census, excluding the names and addresses of those who have requested it, will be published quarterly.

4. A consideration may be required for the provision of this list in computerized form.

Article 32. Type codes.

1. By means of sectoral agreements, administrative agreements or company decisions, those responsible for publicly and privately owned treatment, as well as the organizations in which they are grouped, may draw up standard codes setting out the conditions of organization, operating procedure, Environmental norms, programs or equipment, obligations of those involved in the processing and use of personal information, as well as the guarantees, in its area, for the exercise of the rights of persons with full respect for the principles and provisions Of this Law and its rules of development.

2. These codes may or may not contain detailed operational rules for each particular system and technical application standards.

In the event that such rules or standards are not incorporated directly into the code, the instructions or orders that establish them shall respect the principles set forth therein.

3. The type codes shall have the character of codes of ethics or good professional practice, and shall be deposited or registered in the General Data Protection Register and, where appropriate, in those created for these purposes by the Autonomous Communities, in accordance with Article 41. The General Registry of Data Protection may refuse registration when it considers that it does not comply with the legal and regulatory provisions on the subject, in which case, the Director of the Data Protection Agency must request the To make the necessary corrections.

TITLE V

International data movement

Article 33. General rule.

1. Temporary or definitive transfers of personal data that have been subject to treatment or have been collected for treatment to countries that do not provide a level of protection comparable

to that provided by this Law may not be carried out, unless , In addition to complying with the provisions thereof, obtain prior authorization from the Director of the Data Protection Agency, which may only grant it if adequate guarantees are obtained.

2. The adequacy of the level of protection offered by the country of destination shall be assessed by the Data Protection Agency taking into account all the circumstances of the transfer or category of data transfer. In particular, the nature of the data, the purpose and duration of the intended treatment or treatment, the country of origin and the country of final destination, the general or sectoral legal rules in force in the country The content of the reports of the Commission of the European Union, as well as the professional standards and security measures in force in those countries.

Article 34. Exceptions.

The provisions of the previous article shall not apply:

A) When the international transfer of personal data results from the application of treaties or agreements to which Spain is a party.

B) When the transfer is made for the purpose of providing or requesting international judicial assistance.

C) Where the transfer is necessary for the prevention or for the medical diagnosis, the provision of medical care or treatment or the management of health services.

D) When it refers to monetary transfers according to its specific legislation.

E) When the person concerned has given his unequivocal consent to the proposed transfer.

F) When the transfer is necessary for the execution of a contract between the affected and the person in charge of the file or for the adoption of pre-contractual measures taken at the request of the affected party.

G) Where the transfer is necessary for the execution or execution of a contract concluded or to be concluded, in the interest of the affected, by the person responsible for the file and a third party.

H) When the transfer is necessary or legally required for the safeguarding of a public interest.

This consideration shall be the transfer requested by a tax or customs administration for the fulfillment of its powers.

I) When the transfer is accurate for the recognition, exercise or defense of a right in a judicial process.

J) When the transfer is made, at the request of a person with a legitimate interest, from a public registry and that is in accordance with the purpose of the same.

(K) where the transfer is to a Member State of the European Union, or a State in respect of which the Commission of the European Communities, in the exercise of its powers, has declared that it guarantees an adequate level of protection.

TITLE VI

Data Protection Agency

Article 35. Nature and legal regime.

1. The Data Protection Agency is an entity governed by public law, with its own legal personality and full public and private capacity, which acts in full independence of the Public Administrations in the exercise of their functions. It shall be governed by the provisions of this Law and by its own Statute, which shall be approved by the Government.

2. In the exercise of its public functions, and in the absence of the provisions of this Law and its development provisions, the Data Protection Agency shall act in accordance with Law 30/1992, of November 26, on the Legal System Of the Public Administrations and of the Common Administrative Procedure. In its acquisitions patrimoniales and contracting will be subject to the private law.

3. The positions of the bodies and services that make up the Data Protection Agency shall be carried out by officials of the Public Administrations and by personnel hired for this purpose, depending on the nature of the duties assigned to each job. This staff is obliged to keep secret the personal data of which it knows in the development of its function.

4. The Data Protection Agency shall count, for the fulfillment of its purposes, with the following assets and economic means:

A) Allocations that are established annually from the General State Budget.

B) The assets and values that constitute its patrimony, as well as the products and income of the same.

C) Any other legally attributable.

5. The Data Protection Agency shall prepare and approve the corresponding preliminary draft budget on an annual basis and forward it to the Government to be integrated, with due independence, into the General State Budget.

Article 36. The Director.

1. The Director of the Data Protection Agency shall direct the Agency and represent it. It will be named, among those who make up the Advisory Council, by Royal Decree, for a period of four years.

2. It will exercise its functions with full independence and objectivity and will not be subject to any instruction in the performance of those.

In any case, the Director must listen to the Advisory Council in the proposals that he makes in the exercise of his duties.

3. The Director of the Data Protection Agency shall cease only before the expiry of the period referred to in paragraph 1, at his own request or by a separation agreed by the Government, following a preliminary investigation, in which the Other members of the Advisory Board, for serious breach of their obligations, incapacity for the exercise of their function, incompatibility or conviction for intentional crime.

4. The Director of the Data Protection Agency shall be considered a high-ranking official and shall remain in the position of special services if he or she was previously performing a public function. In the event that a member of the judicial or fiscal career is appointed to the position, he will also go to the administrative situation of special services.

Article 37. Functions.

The functions of the Data Protection Agency are:

A) Ensure compliance with data protection legislation and monitor its application, especially as regards rights to information, access, rectification, opposition and cancellation of data.

B) Issue the authorizations provided for in the Law or in its regulations.

C) Issue, if necessary, and without prejudice to the powers of other organs, the precise instructions to adapt the treatments to the principles of this Law.

D) To respond to the requests and claims made by the people affected.

E) Provide information to individuals about their rights regarding the processing of personal data.

F) To require those responsible and those in charge of the treatments, following their hearing, to take the necessary measures to adapt the data treatment to the provisions of this Law and, if necessary, order the cessation of treatment and The cancellation of the files, when it does not conform to its provisions.

G) Exercise the sanctioning power in the terms provided for in Title VII of this Law.

H) Inform, with a prescriptive character, the draft general provisions that develop this Law.

I) To gather from the file managers what help and information they deem necessary for the performance of their duties.

J) Ensure publicity for the existence of personal data files, for which purpose it shall periodically publish a list of such files with the additional information determined by the Director of the Agency.

K) Write an annual report and send it to the Ministry of Justice.

(L) To exercise control and take appropriate authorizations in relation to international data movements and to perform the functions of international cooperation in the field of personal data protection.

M) Ensure compliance with the provisions established by the Law on the Public Statistical Function with regard to the collection of statistical data and statistical confidentiality, as well as to dictate the precise instructions, to rule on the security conditions of the files constituted exclusively for purposes And exercise the power referred to in Article 46.

N) As many others are attributed to him by legal or regulatory norms.

Article 38. Advisory Council.

The Director of the Data Protection Agency shall be advised by an Advisory Board composed of the following members:

A Deputy, proposed by the Congress of Deputies.

A Senator, proposed by the Senate.

A representative of the Central Administration, appointed by the Government.

A representative of the Local Administration, proposed by the Spanish Federation of Municipalities and Provinces.

A member of the Royal Academy of History, proposed by the same.

An expert on the subject, proposed by the Higher Council of Universities.

A representative of users and consumers, selected in the manner provided for by regulation.

A representative of each Autonomous Community that has created a data protection agency in its territorial scope, proposed in accordance with the procedure established by the respective Autonomous Community.

A representative of the sector of private files, whose proposal will follow the procedure that is regulated by regulations.

The functioning of the Advisory Council shall be governed by the regulatory rules established for this purpose.

Article 39. The General Registry of Data Protection.

1. The General Registry of Data Protection is an organ integrated in the Data Protection Agency.

2. They will be registered in the General Registry of Data Protection:

A) The files held by the Public Administrations.

B) Private ownership files.

C) The authorizations referred to in this Law.

D) The type codes referred to in article 32 of this Law.

E) The data related to the files that are necessary for the exercise of the rights of information, access, rectification, cancellation and opposition.

3. The registration procedure for the files, both publicly owned and privately owned, will be regulated by the regulatory procedure, the contents of the registration, modification, cancellation, complaints and appeals against resolutions Corresponding points and other relevant points.

Article 40. Power of inspection.

1. The control authorities may inspect the files referred to in this Law, collecting all the information they need to carry out their duties.

For this purpose, they may request the display or the sending of documents and data and examine them at the place where they are deposited, as well as inspect the physical and logical equipment used for the processing of the data, accessing the premises where they are installed .

2. The officials who carry out the inspection referred to in the previous section shall be considered public authority in the performance of their duties.

They will be obliged to keep secret on the information they know in the exercise of the mentioned functions, even after they have ceased in the same.

Article 41. Corresponding bodies of the Autonomous Communities.

1. The functions of the Data Protection Agency regulated in article 37, with the exception of those mentioned in sub-paragraphs (j), (k) and (l), and in subparagraphs (f) and (g) Of data, as well as in articles 46 and 49, in relation to their specific powers will be exercised, when they affect personal data files created or managed by the Autonomous Communities and by the Local Administration of its territorial scope, by the bodies Which shall be considered as supervisory authorities, to which they shall guarantee full independence and objectivity in the performance of their duties.

2. The Autonomous Communities may create and maintain their own records of files for the exercise of the competences that are recognized on them.

3. The Director of the Data Protection Agency may convene regularly to the corresponding bodies of the Autonomous Communities for the purpose of institutional cooperation and coordination of criteria or procedures for action. The Director of the Data Protection Agency and the corresponding bodies of the Autonomous Communities may request each other the information necessary for the performance of their duties.

Article 42. Files of the Autonomous Communities in matters of their exclusive competence.

1. When the Director of the Data Protection Agency finds that the maintenance or use of a specific file of the Autonomous Communities contravenes any provision of this Law in respect of its exclusive competence may request the corresponding Administration to take corrective measures That determines in the term that expressly is fixed in the request.

2. If the corresponding public administration fails to comply with the request, the Director of the Data Protection Agency may challenge the decision adopted by that Administration.

TITLE VII

Offenses and penalties

Article 43. Responsible.

1. Those responsible for the files and those in charge of the treatments will be subject to the sanctioning regime established in this Law.

2. In the case of files for which the Public Administrations are responsible, the provisions of Article 46 (2) shall apply in respect of procedure and penalties.

Article 44. Types of infractions.

1. Offenses shall be classified as minor, serious or very serious.

2. They are minor infractions:

A) Do not attend, for formal reasons, the request of the interested party to rectify or cancel the personal data being processed when legally appropriate.

B) Failure to provide the information requested by the Data Protection Agency in the exercise of the powers it has legally attributed, in relation to non-substantive aspects of data protection.

C) Not request the registration of the personal data file in the General Data Protection Registry, when it does not constitute a serious infringement.

D) Proceed with the collection of personal data of the affected persons without providing them with the information indicated in article 5 of this Law.

E) To breach the duty of secrecy established in article 10 of this Law, unless it constitutes a serious infraction.

3. Serious offenses:

A) Proceed with the creation of files of public ownership or initiate the collection of personal data for them, without authorization of general provision, published in the "Official State Gazette" or corresponding official Journal.

B) Proceed with the creation of files of private ownership or initiate the collection of personal data for them with purposes other than those that constitute the legitimate object of the company or entity.

C) To proceed with the collection of personal data without obtaining the express consent of the affected persons, in cases in which it is demandable.

D) To treat personal data or to use them subsequently in violation of the principles and guarantees established in this Law or in breach of the precepts of protection imposed by the regulatory development provisions, when it does not constitute a very serious violation.

E) The impediment or obstruction of the exercise of the rights of access and opposition and the refusal to provide the information that is requested.

F) To maintain inaccurate personal data or not to make corrections or cancellations of the same that legally proceed when they affect the rights of the people that this Law covers.

G) The breach of the duty to keep secret personal data incorporated in files containing data relating to the commission of administrative or criminal offenses, Public Finance, financial services, provision of creditworthiness and credit services, as well as those others Files containing a set of personal data sufficient to obtain an assessment of the personality of the individual.

H) Keep the files, premises, programs or equipment containing personal data without due security conditions that are determined by regulation.

I) Do not send to the Data Protection Agency the notifications provided for in this Law or in its development provisions, as well as not provide in time to the same as all documents and information must receive or are required by the same for such purposes.

J) The obstruction to the exercise of the inspection function.

K) Not register the personal data file in the General Registry of Data Protection, when it has been requested by the Director of the Data Protection Agency.

L) Failure to fulfill the duty of information established in articles 5, 28 and 29 of this Law, when the data have been collected from a person other than the affected.

4. These are very serious offenses:

A) The collection of data in a deceptive and fraudulent way.

B) The communication or transfer of personal data, outside the cases in which they are allowed.

C) Collect and process the personal data referred to in article 7, paragraph 2, when the express consent of the affected person does not exist; Collect and process the data referred to in Article 7 (3) when not provided for by law or the person concerned has not expressly consented to or violates the prohibition contained in Article 7 (4).

D) Not cease in the illegitimate use of the processing of personal data when required by the Director of the Data Protection Agency or by the persons holding the right of access.

E) The temporary or definitive transfer of personal data that have been processed or have been collected to be subjected to such treatment, to countries that do not provide a comparable level of protection without authorization from the Director of the Protection Agency Data.

F) To treat personal data illegitimately or with contempt of the principles and guarantees applicable to them, when this is prevented or threatened against the exercise of fundamental rights.

G) Infringement of the duty to keep secret the personal data referred to in paragraphs 2 and 3 of article 7, as well as those that have been collected for police purposes without the consent of the affected persons.

H) Do not attend, or systematically obstruct the exercise of rights of access, rectification, cancellation or opposition.

I) Not systematically attending to the legal duty of notification of the inclusion of personal data in a file.

Article 45. Type of sanctions.

1. Minor infractions will be sanctioned with a fine of 100,000 to 10,000,000 pesetas.

2. Serious infringements shall be punishable by a fine of between 10,000,000 and 50,000,000 pesetas.

3. Very serious infractions will be sanctioned with a fine of 50,000,000 to 100,000,000 pesetas.

4. The amount of the sanctions shall be graduated taking into account the nature of the personal rights affected, the volume of the treatments carried out, the benefits obtained, the degree of intentionality, the recidivism, the damages caused to the persons concerned And to any other circumstance that is relevant to determine the degree of anti-legality and guilt present in the specific infraction.

5. If, as a result of the circumstances in question, a qualified diminution of the culpability of the accused or of the unlawfulness of the act is detected, the sanctioning body shall establish the amount of the penalty by applying the scale relating to the class of infractions that immediately precedes in Seriousness to that in which the considered in the case in question is integrated.

6. In no case may a more serious sanction be imposed than the one established in the Law for the class of infraction in which it is integrated the one that is intended to sanction.

7. The Government will periodically update the amount of sanctions in accordance with variations in price indices.

Article 46. Offenses of Public Administrations.

1. Where the offenses referred to in Article 44 are committed in files for which the Public Administrations are responsible, the Director of the Data Protection Agency shall issue a decision establishing the measures to be taken to cease or Effects of the infringement.

This resolution will be notified to the person in charge of the file, to the organ of which it depends hierarchically and to the affected ones if any.

2. The Director of the Agency may also propose the initiation of disciplinary proceedings, if applicable.

The procedure and penalties to be applied shall be those established in the legislation on the disciplinary regime of the Public Administrations.

3. Resolutions relating to the measures and actions referred to in the preceding paragraphs shall be communicated to the Agency.

4. The Director of the Agency shall inform the Ombudsman of the actions he has taken and the resolutions he makes pursuant to the preceding paragraphs.

Article 47. Prescription.

1. Very serious offenses shall be prescribed at three years, serious at two years and minor at one year.

2. The limitation period shall begin to run from the day on which the offense was committed.

3. The limitation shall be interrupted by the initiation, with the knowledge of the interested party, of the sanctioning procedure, resumption of the limitation period if the sanctioning file is paralyzed for more than six months for causes not attributable to the alleged offender.

4. The penalties imposed for very serious offenses shall be imposed at three years, those imposed for serious offenses at two years and those imposed for minor offenses per year.

5. The limitation period for penalties shall begin to run from the day following that in which the decision imposing the sanction becomes final.

6. The limitation period shall be interrupted by the initiation, with the knowledge of the interested party, of the execution procedure, and the deadline will be exceeded if it is paralyzed for more than six months for a cause not attributable to the offender.

Article 48. Sanctioning procedure.

1. The procedure to be followed for the determination of infringements and the imposition of the sanctions referred to in this Title shall be established by means of a regulatory procedure.

2. The resolutions of the Data Protection Agency or corresponding body of the Autonomous Community exhaust the administrative route.

Article 49. Power of immobilization of files.

In the cases that constitute a very serious infringement, the use or unlawful transfer of personal data in which it is seriously impeded or similarly jeopardized against the exercise of the rights of citizens and the free development of the personality that the Constitution and the laws guarantee, the Director of the Data Protection Agency may, in addition to exercising the sanctioning power, require those responsible for files of personal data, both public and private ownership, cessation in the use or assignment Of the data. If the request is disregarded, the Data Protection Agency may, by means of a reasoned resolution, immobilize such files for the sole purpose of restoring the rights of the persons concerned.

Additional provision one. Pre-existing files.

The files and automated treatments registered or not in the General Registry of Data Protection must comply with this Organic Law within a period of three years, starting from its entry into force.

Within this period, privately owned files must be communicated to the Data Protection Agency and public administrations, responsible for publicly owned files, must approve the relevant regulatory provision of the file or adapt the existing one.

In the case of non-automated files and treatments, their adaptation to this Organic Law, and the obligation set forth in the previous paragraph, must be completed within a period of twelve years starting on October 24, 1995, without prejudice to the exercise of Access rights, rectification and cancellation by those affected.

Second additional provision. Files and Population Register of Public Administrations.

1. The General Administration of the State and the Administrations of the Autonomous Communities may request from the National Statistical Institute, without the consent of the interested party, an updated copy of the file consisting of the name, surname, address, sex and date of birth In the municipal registers of inhabitants and in the electoral census corresponding to the territories where they exercise their powers, for the creation of files or registers of population.

2. The files or registers of population will have as purpose the communication of the different organs of each Public Administration with the interested parties residing in the respective territories, with respect to the administrative legal relationships derived from the respective competences of the Public Administrations.

Third Additional Provision. Treatment of the files of the repealed Laws of Vagos and Maleantes and of Hazard and Social Rehabilitation.

The files specifically instructed under the repealed Laws of Vagos and Maleantes, and of Dangerousness and Social Rehabilitation, containing data of any kind that may affect the security, honor, privacy or the image of the people, may not Be consulted without the express consent of the persons concerned, or fifty years have elapsed since their date.

In this latter case, the General State Administration, unless there is an express record of the death of the affected persons, will make the documentation available to the applicant, removing the data referred to in the previous paragraph, using the relevant technical procedures in each case.

Additional provision four. Modification of article 112.4 of the General Tax Law.

The fourth section of Article 112 of the General Tax Law is now worded as follows:

"4. The assignment of personal data, subject to treatment, that must be made to the Tax Administration in accordance with the provisions of article 111, in the previous paragraphs of this article or another legal standard, will not require The consent of the person concerned.

In this area it will not be applicable what the Public Administrations establishes article 21 (1) of the Organic Law on Personal Data Protection. "

Additional fifth provision. Competences of the Ombudsman and similar autonomous bodies.

The provisions of this Organic Law are understood without prejudice to the powers of the Ombudsman and the analogous bodies of the Autonomous Communities.

Additional provision sixth. Modification of article 24.3 of the Law on Planning and Supervision of Private Insurance.

Article 24.3, paragraph 2 of Law 30/1995, of November 8, on the Management and Supervision of Private Insurance, is modified, with the following wording:

"The insurance companies may establish common files containing personal data for the settlement of claims and actuarial statistical collaboration in order to allow the pricing and selection of risks and the preparation of studies of insurance technique.

The transfer of data to the aforementioned files will not require the prior consent of the affected party, but the communication to the same of the possible transfer of their personal data to common

files for the purposes indicated with express indication of the responsible one so that the rights of Access, rectification and cancellation provided for by law.

Common files may also be established whose purpose is to prevent fraud in the insurance without the consent of the affected party being necessary. However, it will be necessary in these cases to communicate to the affected, in the first introduction of their data, who is responsible for the file and the ways of exercising rights of access, rectification and cancellation.

In any case, health data may only be processed with the express consent of the person concerned. "

First transitional provision. Treatments created by international conventions.

The Data Protection Agency shall be the body competent for the protection of natural persons with regard to the processing of personal data in respect of the treatments established in any International Convention of which Spain is a party, attributing to a national control authority Until such time as a different authority is created for this role in the development of the Convention.

Second transitory provision. Use of the promotional census.

The procedures for the formation of the promotional census, of opposition to appear in the same, of making available to its applicants, and of control of the disseminated lists will be regulated.

The Regulation will establish the deadlines for the implementation of the promotional census.

Transitional Provision Three. Subsistence of pre-existing standards.

Until such time as the provisions of the first final provision of this Law are carried out, the existing regulations and, in particular, Royal Decrees 428/1993 of 26 March shall continue to be in force, with their own rank; 1332/1994 of June 20 and 994/1999 of June 11, insofar as they do not oppose this Law.

Single derogatory provision. Normative repeal.

The Organic Law 5/1992, of October 29, regulating the automated processing of personal data is hereby repealed.

Final disposition first. Enabling for regulatory development.

The Government will approve, or modify, the necessary regulatory dispositions for the application and development of this Law.

Second final provision. Precepts as ordinary law.

Titles IV, VI, except the last paragraph of paragraph 4 of article 36 and VII of this Law, the fourth additional provision, the first transitional provision and the first final have the character of ordinary law.

Third final provision. Entry into force.

This Law shall enter into force within a period of one month, counted from its publication in the "Official State Gazette".

So,

I command all Spaniards, individuals and authorities, to keep and keep this Organic Law.

Madrid, December 13, 1999.

JUAN CARLOS R.

The president of the Government,
JOSÉ MARÍA AZNAR LÓPEZ

Analysis

- Rank: Organic Law
- Date of readiness: 12/13/1999
- Date of publication: 12/14/1999
- Entry into force: January 14, 2000.

Subsequent references

Management Criteria: **By content** **by date**

- The arts. 43 to 46, by Law 2/2011, of March 4 (Ref. BOE-A-2011-4117).
- IS DEVELOPED, by Royal Decree 1720/2007, of 21 December (Ref. BOE-A-2008-979).
- IT IS DECIDED TO COMPLY:
    - On the processing of personal data for the purposes of surveillance through camera or video camera systems: Instruction 1/2006, of 8 November (Ref. BOE-A-2006-21648).
    - With the art. 37.2, on publication of the resolutions of the Data Protection Agency: Instruction 1/2004, of 22 December (Ref. BOE-A-2005-186).
- The arts. 37 and 48, by Law 62/2003, of December 30 (Ref. BOE-A-2003-23936).
- IT IS UPDATED, on conversion into euros of the amounts indicated: Resolution of 11 December 2001 (Ref. BOE-A-2001-24149).
- DECLARED in REMEDY 1463/2000, the unconstitutionality and nullity of the indicated paragraphs of arts. 21.1 and 24.1 and 24.2, by Judgment 292/2000, of November 30 (Ref. BOE-T-2001-332).
- IT IS SAYED PURSUANT TO Art. 37.c), on international data movements: Instruction 1/2000, of 1 December (Ref. BOE-A-2000-22726).

Previous references

- DEROGA Organic Law 5/1992, of October 29 (Ref. BOE-A-1992-24189).
- MODIFY:
    - art. 24.3 of Law 30/1995, of November 8 (Ref. BOE-A-1995-24262).
    - art. 112.4 of Law 230/1963, of 28 December (Ref. BOE-A-1963-22706).

Subjects

- Data Protection Agency
- Right of access to data
- Files with personal data

- Sanctioning procedure
- General Data Protection Registry

https://www.boe.es/buscar/doc.php?id=BOE-A-1999-23750