ORGANIC LAW 15/1999 of 13 December on the Protection of Personal Data

This is an unofficial translation that has been updated according to the changes operated in the Act after the Sentence 292/200 of the Spanish Constitutional Court

Please note that the only legally binding text
is that published in the Spanish Official Journal

I. General provisions

OFFICE OF THE HEAD OF STATE

23750 ORGANIC LAW 15/1999 of 13 December on the Protection of Personal Data.

JUAN CARLOS I
KING OF SPAIN

To whom it may concern.
Know ye that Parliament has passed, and I approve, the following Organic Law.

TITLE I

General provisions

Article 1. *Subject*

This Organic Law is intended to guarantee and protect the public liberties and fundamental rights of natural persons, and in particular their personal and family privacy, with regard to the processing of personal data.

Article 2. *Scope*

1. This Organic Law shall apply to personal data recorded on a physical support which makes them capable of processing, and to any type of subsequent use of such data by the public and private sectors.
This Organic Law shall govern any processing of personal data:

a) When the processing is carried out on Spanish territory as part of the activities of an establishment belonging to the person responsible for the processing.
b) When the person responsible for the processing is not established on Spanish territory but is subject to Spanish law pursuant to the norms of public international law.
c) When the person responsible for the processing is not established on the territory of the European Union and is using for the processing means situated on Spanish territory, unless such means are used solely for transit purposes.

2. The system of protection of personal data laid down by this Organic Law shall not apply to:

a) Files maintained by natural persons in the exercise of purely personal or household activities.
b) Files subject to the legislation on the protection of classified materials.
c) Files established for the investigation of terrorism and serious forms of organised crime. However, in such cases, the person responsible for the file shall previously inform the Data Protection Agency of its existence, its general characteristics and its purpose.

3. The following processing of personal data shall be governed by the specific provisions, and by any special provisions, of this Organic Law:

a) Files regulated by the legislation on the electoral system.
b) Those used solely for statistical purposes and protected by central or regional government legislation on public statistical activities.
c) Those intended for the storage of the data contained in the personal assessment reports covered by the legislation on the personnel regulations of the armed forces.
d) Those contained in the Civil Register and the Central Criminal Register.
e) Thos deriving from images and sound recorded by videocameras for the security forces in accordance with the relevant legislation.

Article 3. *Definitions*

The following definitions shall apply for the purposes of this Organic Law:

a) Personal data: any information concerning identified or identifiable natural persons.
b) File: any structured set of personal data, whatever the form or method of its creation, storage organisation and access.
c) Processing of data: operations and technical processes, whether or not by automatic means, which allow the collection, recording, storage, adaptation, modification, blocking and cancellation, as well as assignments of data resulting from communications, consultations, interconnections and transfers.
d) Controller: natural or legal person, whether public or private, or administrative body which determines the purpose, content and use of the processing.
e) Data subject: the natural person who owns the data undergoing the processing referred to in (c) above.
f) Dissociation procedure: any processing of personal data carried out in such a way that the information obtained cannot be associated with an identified or identifiable person.
g) Processor: the natural or legal person, public authority, service or any other body which alone or jointly with others processes personal data on behalf of the controller.
h) Consent of the data subject: any free, unequivocal, specific and informed indication of his wishes by which the data subject consents to the processing of personal data relating to him.
i) Assignment or communication of data: any disclosure of data to a person other than the data subject.
j) Sources accessible to the public: those files which can be consulted by anyone, which are not subject to restrictive legislation, or which are subject only to payment of a consultation fee. Only the following shall be considered to be sources accessible to the public: the publicity register, telephone directories subject to the conditions laid down in the relevant regulations, and the lists of persons belonging to professional associations containing only data on the name, title, profession, activity, academic degree, address and an indication of his membership of the association. Newspapers, official gazettes and the media shall also be considered sources with public access.

TITLE II

Principles of data protection

Article 4. *Quality of the data*

1. Personal data may be collected for processing, and undergo such processing, only if they are adequate, relevant and not excessive in relation to the scope and the specified, explicit and legitimate purposes for which they were obtained.
2. Personal data subjected to processing may not be used for purposes incompatible with those for which they were collected. Further processing of the data for historical, statistical or scientific purposes shall not be considered incompatible.
3. Personal data shall be accurate and updated in such a way as to give a true picture of the current situation of the data subject.
4. If the personal data recorded prove to be inaccurate, either in whole or in part, or incomplete, shall be erased and officially replaced by the corresponding rectified or supplemented data, without prejudice to the rights granted to data subjects in Article 16.
5. Personal data shall be erased when they have ceased to be necessary or relevant for the purpose for which they were obtained or recorded.
They shall not be kept in a form which permits identification of the data subject for longer than necessary for the purposes for which they were obtained or recorded.
On a regular basis, the procedure shall be determined by which, exceptionally, it is decided to keep the entire set of particular data, in accordance with the specific legislation, because of their historical, statistical or scientific value.
6. Personal data shall be stored in a way which permits the right of access to be exercised, unless lawfully erased.
The collection of data by fraudulent, unfair or illicit means is prohibited.

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

1. Data subjects from who personal data are requested must previously be informed explicitly, precisely and unequivocally of the following:

a) The existence of a file or personal data processing operation, the purpose of collecting the data, and the recipients of the information.
b) The obligatory or voluntary nature of the reply to the questions put to them.
c) The consequences of obtaining the data or of refusing to provide them.
d) The possibility of exercising rights of access, rectification, erasure and objection.
e) The identity and address of the controller or of his representative, if any.

Where the controller is not established on the territory of the European Union, and he is using for the processing means situated on Spanish territory, he must, unless these means are being used for transit purposes, designate a representative in Spain, without prejudice to any action which may be taken against the controller himself.
2. Where questionnaires or other forms are used for collection, they must contain the warnings set out in the previous paragraph in a clearly legible form.

3. The information set out in subparagraphs (b), (c) and (d) of paragraph 1 shall not be required if its content can be clearly deduced from the nature of the personal data requested or the circumstances in which they are obtained.
4. Where the personal data have not been obtained from the data subject, he must be informed explicitly, precisely and unequivocally by the controller or his representative within three months from the recording of the data - unless he has been informed previously - of the content of the processing, the origin of the data, and the information set out in (a), (d) and (e) of paragraph 1 of this Article.
5. The provisions of the preceding paragraph shall not apply where explicitly provided for by law, when the processing is for historical, statistical or scientific purposes, or when it is not possible to inform the data subject, or where this would involve a disproportionate effort in the view of the Data Protection Agency or the corresponding regional body, in view of the number of data subjects, the age of the data and the possible compensatory measures.
The provisions of the preceding paragraph shall also not apply where the data come from sources accessible to the public and are intended for advertising activity or market research, in which case each communication sent to the data subject shall inform him of the origin of the data, the identity of the controller and the rights of the data subject.

Article 6. *Consent of the data subject*

1. Processing of personal data shall require the unambiguous consent of the data subject, unless laid down otherwise by law.
2. Consent shall not be required where the personal data are collected for the exercise of the functions proper to public administrations within the scope of their responsibilities; where they relate to the parties to a contract or preliminary contract for a business, employment or administrative relationship, and are necessary for its maintenance or fulfilment; where the purpose of processing the data is to protect a vital interest of the data subject under the terms of Article 7(6) of this Law, or where the data are contained in sources accessible to the public and their processing is necessary to satisfy the legitimate interest pursued by the controller or that of the third party to whom the data are communicated, unless the fundamental rights and freedoms of the data subject are jeopardised.
3. The consent to which the Article refers may be revoked when there are justified grounds for doing so and the revocation does not have retroactive effect.
4. In the cases where the consent of the data subject is not required for processing personal data, and unless provided otherwise by law, the data subject may object to such processing when there are compelling and legitimate grounds relating to a particular personal situation. In such an event, the controller shall exclude the data relating to the data subject from the processing.

Article 7. *Data with special protection*

1. In accordance with the provisions of Article 16(2) of the Constitution, nobody may be obliged to state his ideology, religion or beliefs.
If, in relation to such data, the consent referred to in the following paragraph is sought, the data subject shall be warned of his right to refuse such consent.
2. Personal data which reveal the ideology, trade union membership, religion and beliefs may be processed only with the explicit and written consent of the data subject. Exceptions shall be files maintained by political parties, trade unions, churches, religious confessions or communities, and

associations, foundations and other non-profit-seeking bodies with a political, philosophical, religious or trade-union aim, as regards the data relating to their associates or members, without prejudice to the fact that assignment of such data shall always require the prior consent of the data subject.
3. Personal data which refer to racial origin, health or sex life may be collected, processed and assigned only when, for reasons of general interest, this is so provided for by law or the data subject has given his explicit consent.
4. Files created for the sole purpose of storing personal data which reveal the ideology, trade union membership, religion, beliefs, racial or ethnic origin or sex life remain prohibited.
5, Personal data on criminal or administrative offences may be included in files of the competent public administrations only under the circumstances laid down in the respective regulations.
6. Notwithstanding the provisions of the preceding paragraphs, the personal data referred to in paragraphs 2 and 3 of this Article may be processed when such processing is necessary for purpose of preventive medicine or diagnosis, the provision of medical care or treatment, or the management of health-care services, provided such data processing is effected 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 preceding subparagraph may also be processed when this is necessary to safeguard the vital interests of the data subject or another person in the event that the data subject is physically or legally incapable of giving his consent.

Article 8. *Data on health*

Without prejudice to the provisions of Article 11 on assignment, public and private health-care institutions and centres and the corresponding professionals may process personal data relating to the health of persons consulting them or admitted to them for treatment, in accordance with the provisions of the central or regional government legislation on health care.

Article 9. *Data security*

1. The controller or, where applicable, the processor shall adopt the technical and organisational measures necessary to ensure the security of the personal data and prevent their alteration, loss, unauthorised processing or access, having regard to the state of the art, the nature of the data stored and the risks to which they are exposed by virtue of human action or the physical or natural environment.
2. No personal data shall be recorded in files which do not meet the conditions laid down by rules regarding their integrity and security, as well as the rules governing the processing centres, premises, equipment, systems and programs.
3. Rules shall be laid down governing the requirements and conditions to be met by the files and the persons involved in the data processing referred to in Article 7 of this Law.

Article 10. *Duty of secrecy*

The controller and any persons involved in any stage of processing personal data shall be subject to professional secrecy as regards such data and to the duty to keep them. These obligations shall continue even after the end of the relations with the owner of the file or, where applicable, the person responsible for it.

Article 11. *Communication of data*

1. Personal data subjected to processing may be communicated to third persons only for purposes directly related to the legitimate functions of the transferor and transferee with the prior consent of the data subject.
2. The consent required under the previous paragraph shall not be required:
a) when the transfer is authorised by a law.
b) when the data have been collected from publicly accessible sources.
c) when the processing corresponds to the free and legitimate acceptance of a legal relationship whose course, performance and monitoring necessarily involve the connection between such processing and files of third parties. In that case, communication shall be legitimate to the extent of the purpose justifying it.
d) when the communication to be effected is destined for the Ombudsman, the Office of Public Prosecutor, judges, courts or the Court of Auditors in the exercise of the functions assigned to them. Not shall consent be required when the communication is destined to regional government authorities with functions analogous to the Ombudsman or the Court of Auditors.
e) when the transfer is between public administrations and concerns the retrospective processing of the data for historical, statistical or scientific purposes.
f) when the transfer of personal data on health is necessary for resolving an emergency which requires access to a file or for conducting epidemiological studies within the meaning of central or regional government health legislation.
3. Consent for the communication of personal data to a third party shall be null and void when the information given to the data subject does not enable him to know the purpose for which the data whose communications is authorised will be used or the type of activity of the person to whom it is intended to communicate them.
4. Consent for the communication of personal data may also be revoked.
5. The person to who personal data are communicated is obliged, by the mere fact of the communication, to abide by the provisions of this Law.
6. If the communication is preceded by a depersonalisation procedure, the provisions of the preceding paragraphs shall not apply.

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

1. Access to data by a third party shall not be considered communication of data when such access is necessary for the provision of a service to the data controller.
2. Processing on behalf of third parties shall be regulated in a contract which must be in writing or in any other form which allows its performance and content to be assessed, it being expressly laid down that the processor shall process the data only in accordance with the instructions of the controller, shall not apply or use them for a purpose other than that set out in the said contract, and shall not communicate them to other persons even for their preservation.
The contract shall also set out the security measures referred to in Article 9 of this Law, which the processor is obliged to implement.
3. Once the contractual service has been provided, the personal data must be destroyed or returned to the controller, together with any support or documents contain personal data processed.
4. If the processor uses the data for another purpose, communicates them or uses them in a way not in accordance with the terms of the contract, he shall also be considered as the controller and shall be personally responsible for the infringements committed by him.

TITLE III

Rights of persons

Article 13. *Challenging assessments*

1. Citizens have the right not to be subject to a decision with legal consequences for them, or which significantly affects them, and which is based processing of data intended to assess certain aspects of their personality.
2. The data subject may challenge administrative acts or private decisions which involve an assessment of his behaviour, the only basis for which is the processing of personal data which provides a definition of his characteristics or personality.
3. In that case, the data subject shall have the right to obtain information from the controller on the assessment criteria and program used in the processing on the basis of which the decision containing the act was adopted.
4. An assessment of the behaviour of citizens based on data processing shall have conclusive force only at the request of the data subject.

Article 14. *Right to consult the General Data Protection Register*

Anyone may consult the General Data Protection Register to learn about the existence of personal data, their purpose and the identity of the controller. The General Register shall be open to public consultation free of charge.

Article 15. *Right of access*

1. The data subject shall have the right to request and obtain free of charge information on his personal data subjected to processing, on the origin of such data and on their communication or intended communication.
2. The information may be obtained by simply displaying the data for consultation or by indicating the data subjected to processing in writing, or in a copy, fax or photocopy, whether certified a true copy or not, in legible and intelligible form, and without using keys or codes which require the use of specific devices.
3. The right of access referred to in this Article may be exercised only at intervals of not less than twelve months, unless the data subject can prove a legitimate interest in doing so, in which case it may be exercised before then.

Article 16. *Right of rectification or cancellation*

The controller shall be obliged to implement the right of rectification or cancellation of the data subject within a period of ten days.
2. Rectification or cancellation shall apply to data whose processing is not in accordance with the provisions of this Law and, in particular, when such data are incorrect or incomplete.
3. Cancellation shall lead to the data being blocked and maintained solely at the disposal of the public administrations, judges and courts, for the purpose of determining any liability arising from the processing, and for the duration of such liability. On expiry of such liability, they shall be deleted.

4. If the data rectified or cancelled have previously been communicated, the controller shall notify the person to whom they have been communicated of the rectification or cancellation. If the processing is being maintained by that person, he shall also cancel the data.
5. Personal data shall be kept for the periods set out in the relevant provisions or, where applicable, in the contractual relations between the person or body responsible for the processing ("the controller") and the data subject.

Article 17. *Objection, access, rectification or cancellation procedure*

1. The procedures for exercising the right of objection, access, rectification and cancellation shall be established by regulation.
2. No consideration shall be demanded for the exercise of the rights of objection, access, rectification or cancellation.

Article 18. *Supervision of rights*

1. Acts contrary to the provisions of this Law may be the subject of complaints by data subjects to the Data Protection Agency in the form laid down by regulation.
2. A data subject who is denied, either wholly or partially, the exercise of the rights of objection, access, rectification or cancellation, may bring this to the attention of the Data Protection Agency or, where applicable, to the competent body in each Autonomous Community, which must decide on the admissibility or inadmissibility of the denial.
3. The maximum period within which a decision on the ownership of data must be reached shall be six months.
4. An appeal may be lodged against the decisions of the Data Protection Agency.

Article 19. *Right to damages*

1. Data subjects who, as a result of failure to comply with the provisions of this Law on the part of the controller or processor, suffer damage to their possessions or rights, shall have the right to damages.
2. Where the files are in public ownership, liability shall be established in accordance with the legislation regulating the liability of public administrations.
3. In the case of files in private ownership, the case shall be heard by the civil courts.

TITLE IV

Sectoral provisions

CHAPTER I

Files in public ownership

Article 20. *Creation, modification or deletion*

1. Files of the public administrations may only be created, modified or deleted by means of a general provision published in the *Boletín Oficial del Estado* or in the corresponding official gazette.

2. The provisions for the creation or modification of files must indicate:

a) The purpose of the file and its planned use.
b) The persons or bodies on which it is planned to obtain personal data or which they are obliged to submit data.
c) The procedure for collecting the personal data.
d) The basic structure of the file and a description of the personal data included in it.
e) The intended transfers of personal data and, where applicable, the intended transfers of data to third countries.
f) The officials in the administrations responsible for the file.
g) The services or units with which the rights of access, rectification, cancellation and objection may be exercised.
h) The security measures, indicating the basic, medium or high level required.

3. The provisions on the deletion of files shall lay down the fate of the files or, where applicable, the timetables to be adopted for their destruction.

Article 21. *Communication of data between public administrations*

1. Personal data collected or drawn up by public administrations in the performance of their tasks shall not be communicated to other public administrations for the exercise of different powers or powers relating to other matters unless the communication is for the purpose of subsequent processing for historical, statistical or scientific purposes.
2. Personal data which a public administration obtains or draws up on behalf of another administration may be communicated.
3. Notwithstanding the provisions of Article 11.2.b), communication of data obtained from sources accessible to the public shall apply to files in private ownership only with the consent of data subject or when a law stipulates otherwise.
4. In the cases provided for in paragraphs 1 and 2 of this Article, the consent of the data subject referred to in Article 11 of this Law shall not be required.

Article 22. *Files of the security forces*

1. The files created by the security forces and containing personal data which, because they were collected for administrative purposes, must be recorded permanently, shall be subject to the general rules of this Law.
2. Collection and processing, for police purposes, of personal data by the security forces without the consent of the data subjects shall be limited to those cases and categories of data necessary for the prevention of a genuine threat to public safety or for the suppression of crime; such data shall be stored in special files established for the purpose, which must be classified according to their degree of reliability.
3. The data referred to in paragraphs 2 and 3 of Article 7 may be collected and processed only in cases in which it is absolutely essential for the purposes of a specific investigation, without prejudice to checks on the legality of the administrative action or the obligation to consider any applications made by the data subjects falling within the remit of the bodies responsible for the administration of justice.
4. Personal data stored for police purposes shall be cancelled when they are not necessary for the investigations for the purposes of which they were stored.

To this end, special consideration shall be given to the age of the data subject and the nature of the data stored, the need to maintain the data until the conclusion of a specific investigation or procedure, a final judgment, and in particular an acquittal, a pardon, rehabilitation and the expiry of liability

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

1. The controllers of files containing the data referred to in paragraphs 2, 3 and 4 of the preceding Article may deny access, rectification or cancellation in the light of the risks which might arise for the defence of the state or public safety, the protection of the rights and liberties of third parties, or for the needs of investigations under way.
2. Controllers of files in the public finance sector may also deny exercise of the rights referred to in the previous paragraph when this impede administrative actions aimed at ensuring fulfilment of tax obligations, and particularly when the data subject is under investigation.
3. A data subject who is denied, either wholly or partially, exercise of the rights referred to in the preceding paragraphs may bring this to the notice of the Director of the Data Protection Agency, or of the competent body in each Autonomous Community in the case of files maintained by its own police forces, or the tax authorities of the Autonomous Communities, which must establish the admissibility or inadmissibility of the denial.

Article 24. *Other exceptions to the rights of data subjects*

The provisions of paragraphs 1 and 2 of Article 5 shall not apply to the collection of data when informing the data subject would affect national defence, public safety or the prosecution of criminal offences.

CHAPTER II

Files in private ownership

Article 25. *Creation*

Files in private ownership containing personal data may be created when it is necessary for the success of the legitimate activity and purpose of the person, undertaking or body owning them and the guarantees laid down by this Law for the protection of persons are respected.

Article 26. *Notification and entry in the register*

1. Any person or body creating files of personal data shall first notify the Data Protection Agency,
2. Detailed rules shall be established for the information to be contained in the notification, amongst which must be the name of the controller, the purpose of the file, its location, the type of personal data contained, the security measures, with an indication of whether they are of basic, medium or high level, any transfers intended and, where applicable, ant intended transfers of data to third countries.
3. The Data Protection Agency must be informed of any changes in the purpose of the computer file, the controller and the address of its location.
4. The General Data Protection Register shall enter the file if the notification meets the requirements.
If this is not the case, it may ask for the missing data to be provided or take remedial action.
5. If one month has passed since submitting the application for entry without the Data Protection Agency responding, the computer file shall, for all accounts and purposes, be considered entered in the Register.

Article 27. *Communication of transfers of data*

1. When making the first transfer of data, the controller must communicate this to the data subjects, also indicating the purpose of the file, the nature of the data transferred and the name and address of the transferee.
2. The obligation set out in the preceding paragraph shall not apply in the case provided for in paragraphs 2.c), d) and e) and 6 of Article 11, nor when the transfer is forbidden by law.

Article 28. *Data included in sources accessible to the public*

1. Personal data contained in the publicity register or in the lists of persons belonging to professional associations referred to in Article 3.j) of this Law must be limited to those that are strictly necessary to fulfil the purpose for which each list is intended. The inclusion of additional data by the bodies responsible for maintaining these sources shall require the consent of the data subject, which may be revoked at any time.
2. Data subjects shall have the right to require the body responsible for maintaining the lists of professional associations to indicate, free of charge, that their data may not be used for the purposes of publicity or market research.
Data subjects shall have the right to have all the personal data contained in the publicity register excluded, free of charge, by the bodies entrusted with maintaining those sources.
A reply to the application for exclusion of the unnecessary information or for inclusion of the objection to the use of the data for the purposes of publicity or distance selling must be given within ten days in the case of information provided via telematic consultation or communication, and in the following edition of the list regardless of the medium on which it is published.
3. Publicly accessible sources published in the form of a book or on any other physical support shall cease to be an accessible source when the new edition is published.
If an electronic version of the list is obtained by telematic means, it shall cease to be a publicly accessible source within one year from the moment it was obtained.
4. Data contained in guides to telecommunications services available to the public shall be governed by the relevant legislation.

Article 29. *Provision of information services on creditworthiness and credit*

1. Providers of information services on creditworthiness and credit may process only personal data obtained from registers and sources accessible to the public and set up for that purpose or based on information provided by the data subject or with his consent.
2. Processing is also allowed of personal data relating to the fulfilment or non-fulfilment of financial obligations provided by the creditor or by someone acting on his behalf. In such cases the data subjects shall be informed, within a period of thirty days from the recording, of those who have recorded personal data in files, with a reference to the data included, and they shall be informed of their right to request information on all of them under the conditions laid down by this Law.
3. In the cases referred to in the two paragraphs above, and at the request of the data subject, the data controller shall communicate to him the data, together with any assessments and appreciations made about him during the previous six months and the name and address of the person or body to whom the data have been disclosed.
4. Only those personal data may be recorded and transferred which are necessary for assessing the economic capacity of the data subjects and which, in the case adverse data, do not go back for more than six years, always provided that they give a true picture of the current situation of the data subjects.

Article 30. *Processing for the purpose of publicity and market research*

1. Those involved in compiling addresses, disseminating documents, publicity, distance selling, market research or other similar activities shall use names and addresses or other personal data when they feature in sources accessible to the public or when they have been provided by the data subjects themselves or with their consent.
2. When the data come from sources accessible to the public, in accordance with the provisions of the second paragraph of Article 5.5 of this Law, each communication sent to the data subject shall indicate the origin of the data and the identity of the controller, as well as the rights available to the data subject.
3. In exercising the right of access, data subjects shall have the right to know the origin of their personal data and the rest of the information referred to in Article 15.
4. Data subjects shall have the right to object, upon request and free of charge, to the processing of the data concerning them, in which case they shall be deleted from the processing and, at their mere request, the information about them contained in the processing shall be cancelled.

Article 31. *Publicity register*

1. Those intending to be involved, either permanently or occasionally, in compiling addresses, disseminating documents, publicity, distance selling, market research or other similar activities, may request from the National Statistical Institute or the equivalent bodies in the Autonomous Communities a copy of the publicity register comprising data on the surnames, forenames and domiciles contained in the electoral roll.
2. Each publicity register list shall be valid for one year. Thereafter, the list shall lose its validity as a publicly accessible source.

3. The procedures by which data subjects may request not to be included in the publicity register shall be governed by regulation. Amongst these procedures, which shall be free of charge for the data subjects, shall be the census document. Every quarter, an updated list of the publicity register shall be published, leaving out the names and addresses of those who have asked to be excluded.
4. A consideration may be required for providing the above list on a digital medium.

Article 32. *Standard codes of conduct*

1. By means of sectoral agreements, administrative agreements or company decisions, publicly and privately-owned controllers and the organisations to which they belong may draw up standard codes of conduct laying down the organisation conditions. The operating rules, the applicable procedures, the safety standards for the environment, programs and equipment, the obligations of those involved in the processing and use of personal information, as well as the guarantees, within their remit, for exercising the rights of the individual in full compliance with the principles and provisions of this Law and its implementing rules.
2. These codes may or may not contain detailed operational rules for each particular system and technical standards for their application.
If these codes are not incorporated directly into the code, the instructions or orders for drawing them up must comply with the principles laid down in the code.
3. The codes must be in the form of codes of conduct or of good professional practice, and must be deposited or entered in the General Data Protection Register and, where appropriate, in the registers set up for this purpose by the Autonomous Communities, in accordance with Article 41. The General Data Protection Register may refuse entry when it considers that the code does not comply with the legal and regulatory provisions on the subject. In such a case, the Director of the Data Protection Agency must require the applicants to make the necessary changes.

TITLE V

International movement of data

Article 33. *General rule*

1. There may be no temporary or permanent transfers of personal data which have been processed or which were collected for the purpose of such processing to countries which do not provide a level of protection comparable to that provided by this Law, except where, in addition to complying with this Law, prior authorisation is obtained from the Director of the Data Protection Agency, who may grant it only if adequate guarantees are obtained.
2. The adequacy of the level of protection afforded by the country of destination shall be assessed by the Data Protection Agency in the light of all the circumstances surrounding the data transfer or category of data transfer. Particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question, the content of the reports by the Commission of the European Union, and the professional rules and security measures in force in those countries.

Article 34. *Derogations*

The provisions of the preceding paragraph shall not apply where:

a) The international transfer of personal data is the result of applying treaties or agreements to which Spain is a party.
b) The transfer serves the purposes of offering or requesting international judicial aid.
c) The transfer is necessary for medical prevention or diagnosis, the provision of health aid or medical treatment, or the management of health services.
d) Where the transfer of data is related to money transfers in accordance with the relevant legislation.
e) The data subject has given his unambiguous consent to the proposed transfer.
f) The transfer is necessary for the performance of a contract between the data subject and the controller or the adoption of precontractual measures taken at the data subject's request.
g) The transfer is necessary for the conclusion or performance of a contract concluded, or to be concluded, in the interest of the data subject, between the controller and a third party.
h) The transfer is necessary or legally required to safeguard a public interest. A transfer requested by a tax or customs authority for the performance of its task shall be considered as meeting this condition.
i) The transfer is necessary for the recognition, exercise or defence of a right in legal proceedings.
j) The transfer takes place at the request of a person with a legitimate interest, from a public register, and the request complies with the purpose of the register.
k) The transfer takes place to a Member State of the European Union or to a country which the Commission of the European Communities, in the exercise of its powers, has declared to ensure an adequate level of protection.

TITLE VI

Data Protection Agency

Article 35. *Nature and legal status*

1. The Data Protection Agency is a body under public law, with its own legal personality and unlimited public and private legal capacity, which acts fully independently of the public administrations in the performance of its tasks. It shall be governed by the provisions of this Law and in a Statute of its own to be approved by the Government.
2. In the exercise of its public functions, and until such time as this Law and its implementing provisions are adopted, the Data Protection Agency shall act in conformity with Law 301992 of 26 November on the Legal Status of Public Administrations and the Common Administrative Procedure. Its acquisitions of assets and contracts shall be governed by private law.
3. The posts in the bodies and services belonging to the Data Protection Agency shall be filled by officials of the public administrations and by staff recruited to this end, in accordance with the functions assigned to each post. The staff is obliged to keep secret any personal data of which they acquire knowledge in the performance of their task.
4. For the performance of its tasks, the Data Protection Agency shall have the following assets and resources:

a) The annual appropriations from the General Government Budget.

b) The goods and assets making up its resources, and any interest from them.
c) Any other resources legally assigned to it.

5. Each year the Data Protection Agency shall draw up and approve the corresponding preliminary draft budget and send it to the Government for incorporation, with due regard to its independence, into the General Government Budget.

Article 36. *The Director*

1. The Director of the Data Protection Agency manages and represents the Agency. He shall be appointed from amongst the members of the Consultative Council, by Royal Decree, for a period of four years.
2. He shall exercise his functions fully independently and objectively and shall not be subject to any instructions thereby.
The Director shall in all cases take note of any proposals the Consultative Council may make to him in the exercise of its functions.
3. The Director of the Data Protection Agency may be removed from office before the end of the period set out in paragraph 1 only at his own request or on the instructions of the Government, after an investigation in which the other members of the Consultative Council must be consulted, for serious infringement of his obligations, inability to exercise his functions, incompatibility or conviction for a criminal offence.
4. The Director of the Data Protection Agency shall be considered as occupying a senior post and shall be governed by the special services régime if he was previously exercising a pubic function. If a member of the judicial or tax career bracket is appointed to the post, he shall also be governed by the special services administrative régime.

Article 37. *Functions*

The functions of the Data Protection Agency are as follows:

a) To ensure compliance with the legislation on data protection and ensure its application, in particular as regards the rights of information, access, rectification, objection and cancellation of data.
b) To issue the authorisations provided for in the Law or in its regulatory provisions.
c) To issue, where applicable, and without prejudice to the remits of other bodies, the instructions needed to bring processing operations into line with the principles of this Law.
d) To consider the applications and complaints from the data subjects.
e) To provide information to persons on their rights as regards the processing of personal data.
f) To require controllers and processors, after having heard them, to take the measures necessary to bring the processing operations into line with this Law and, where applicable, to order the cessation of the processing operation when the cancellation of the files, when the operation does not comply with the provisions of the Law.
g) To impose the penalties set out in Title VII of this Law.
h) To provide regular information on the draft general provisions set out in this Law.
i) To obtain from the data controllers any assistance and information it deems necessary for the exercise of its functions.
j) To make known the existence of files of personal data, to which end it shall regularly publish a list of such files with any additional information the Director of the Agency deems necessary.

k) To draw up an annual report and submit it to the Ministry of Justice.
l) To monitor and adopt authorisations for international movements of data, and to exercise the functions involved in international cooperation on the protection of personal data.
m) To ensure compliance with the provisions laid down by the Law on Public Statistics with regard to the collection of statistical data and statistical secrecy, to issue precise instructions, to give opinions on the security conditions of the files set up for purely statistical purposes, and to exercise the powers referred to in Article 46.
n) Any other functions assigned to it by law or regulation.

Article 38. *Consultative Council*

The Director of the Data Protection Agency shall be assisted by a Consultative Council made up of the following members:

One member of the Congress of Deputies, proposed by the Congress.
One member of the Senate, proposed by the Senate.
One member of the central administration, proposed by the Government.
One member of the local administration, proposed by the Spanish Federation of Municipalities and Provinces.
One member of the Royal Academy of History, proposed by the Academy.
One expert in the field, proposed by the Supreme Council of Universities.
A representative of users and consumers, to be selected according to a method to be laid down by regulation.
One representative of each Autonomous Community which has set up a data protection agency on its territory, to be proposed in accordance with the procedure laid down by the Autonomous Community concerned.
One representative of the private file sector, to be proposed according to the procedure laid down by regulation.

The Consultative Council shall operate in accordance with the regulations laid down for that purpose.

Article 39. *The General Data Protection Register*

1. The General Data Protection Register is a body incorporated into the Data Protection Agency.
2. The following shall be entered in the General Data Protection Register:

a) Files owned by the public administrations.
b) Files in private ownership.
c) The authorisations referred to in this Law.
d) The codes of conduct referred to in Article 32 of this Law.
e) Data relating to files which are necessary for the exercise of the rights of information, access, rectification, cancellation and objection.

3. The procedures for entering the files in public and private ownership in the General Data Protection Register, the content of the entry, its modification, cancellation, complaints and

appeals against the corresponding decisions, and other related matters, shall be laid down by regulation.

Article 40. *Powers of inspection*

1. The supervisory authorities may inspect the files referred to in this Law and obtain any information they require for the performance of their tasks.
To this end, they may require the disclosure or transmission of documents and data and examine them at their place of storage, inspect the hardware and software used to process the data, and obtain access to the premises on which they are located.
2. In the performance of their tasks, the officials carrying out the inspection referred to in the preceding paragraph shall be deemed to be a public authority.
They shall be obliged to keep secret any information acquired in the exercise of the aforementioned functions, even after they have ceased to exercise them.

Article 41. *Corresponding bodies of the Autonomous Communities*

1. The functions of the Data Protection Agency set out in Article 37, with the exception of those referred to in paragraphs j), k) and l), and in paragraphs f) and g) as regards international transfers of data, as well as in Articles 46 and 49 relating to its specific powers, shall, when they concern files of personal data created and administered by the Autonomous Communities and by local government within its territory, be exercised by the corresponding bodies in each Community, which shall be deemed to be supervisory authorities guaranteed full independence and objectivity in the performance of their task.
2. The Autonomous Communities may create and maintain their own registers of files for the exercise of the powers assigned to them.
3. The Director of the Data Protection Agency may regularly meet the corresponding bodies in the Autonomous Communities for the purposes of institutional cooperation and coordination of the criteria or operating procedures. The Director of the Data Protection Agency and the corresponding bodies in the Autonomous Communities may ask each other for the information needed for the exercise of their functions.

Article 42. *Files of the Autonomous Communities for which the Agency has sole responsibility*

1. When the Director of the Data Protection Agency establishes that the maintenance or use of a particular file of the Autonomous Communities contravenes any provision of this Law for which it has sole responsibility, he may require the corresponding administration to adopt the corrective measures specified by him within the period laid down by him.
2. If the public administration in question does not comply with the requirement, the Director of the Data Protection Agency may challenge the decision taken by that administration.

TITLE VII

Infringements and penalties

Article 43. *Controllers*

1. Controllers and processors shall be subject to the penalties set out in this Law.
2. In the case of files for which the public administrations are responsible, the provisions of Article 46(2) shall apply to the procedure and penalties.

Article 44. *Types of infringement*

1. Infringements shall be classified as minor, serious and very serious.
2. The following shall be minor infringements:

a) Failure to respond, for formal reasons, to a request by a data subject for the rectification or cancellation of personal data subject to processing, when that request is justified in law.
b) Failure to provide the information requested by the Data Protection Agency in the exercise of the functions assigned to it by law, with regard to non-substantive aspects of data protection.
c) Failure to request the entry of the file of personal data in the General Data Protection Register, where this does not amount to a serious infringement.
d) Collection of personal data on data subjects without providing them with the information set out in Article 5 of this Law.
e) Failure to respect the duty of secrecy set out in Article 10 of this Law, where this does amount to a serious infringement.

3. The following shall be serious infringements:

a) Creating files in public ownership, or initiating the collection of personal data for such files, without the authorisation published in the *Boletín Oficial del Estado* or the corresponding official gazette.
b) Creating files in private ownership, or initiating the collection of data for such files, for purposes other than the legitimate purposes of the undertaking or body.
c) Collecting personal data without obtaining the explicit consent of the data subjects, where this has to be obtained.
d) Processing personal data or subsequently using them in infringement of the principles and guarantees laid down in this Law, and failure to respect the protection laid down by the implementing provisions, where this does not amount to a very serious infringement.
e) Preventing or hindering the exercise of the rights of access and objection, and refusing to provide the information asked for.
f) Maintaining incorrect personal data or failure to rectify or cancel such data when legally obliged if the citizens' rights protected by this Law are affected
g) Breach of the duty of secrecy for personal data incorporated into files containing data on the commission of administrative or criminal offences, public finance, financial services, provision of creditworthiness and credit services, as well as other files containing a set of personal data sufficient to obtain an assessment of the personality of the individual.
h) Maintaining files, premises, programs or hardware containing personal data without the security required by regulations.
i) Failure to send the Data Protection Agency the notifications laid down in this Law or in its implementing provisions, and not providing it, on time, with any documents and information due to it or which it may require to that end.
j) Impeding inspections.
k) Failure to enter a file of personal data in the General Data Protection Register when this has been required by the Director of the Data Protection Agency.

l) Failure to comply with the duty of information laid down in Articles 5, 28 and 29 of this Law, when the data have been obtained from a person other than the data subject.

4. The following shall be very serious infringements:

a) The misleading or fraudulent collection of data.
b) Communication or transfer of personal data other than in cases where these are allowed.
c) Obtaining and processing the personal data referred to in paragraph 2 of Article 7 without the explicit consent of the data subject; obtaining and processing the data referred to in paragraph 3 of Article 7 when not covered by a law or when the data subject has not given his explicit consent, or breaching the prohibition contained in paragraph 4 of Article 7.
d) Failure to cease the illegitimate use of personal data processing operations when required to do so by the Director of the Data Protection Agency or by the persons owning the rights of access.
e) The temporary or final transfer of personal data which have been subjected to processing, or which have been collected for such processing, to countries which do not provide a comparable level of protection, without the authorisation of the Director of the Data Protection Agency.
f) Processing personal data illegally or in breach of the principles and guarantees applying to them, when this prevents or infringes the exercise of fundamental rights.
g) Breach of the duty to maintain the secrecy of the personal data referred to in paragraphs 2 and 3 of Article 7, as well as of data obtained for police purposes without the consent of the data subjects.
h) Systematically impeding or failing to comply with the exercise of the rights of access, rectification, cancellation or objection.
i) Systematic failure to comply with the duty to notify the inclusion of personal data in a file.

Article 45. *Penalties*

1. Minor infringements shall be punished by a fine of Ptas 100 000 to 10 000 000.
2. Serious infringements shall be punished by a fine of Ptas 10 000 000 to 50 000 000.
3. Very serious infringements shall be punished by a fine of Ptas 50 000 000 to 100 000 000.
4. The amount of the penalties shall be graded taking account the nature of the personal rights involved, the volume of the processing operations carried out, the profits gained, the degree of intentionality, repetition, the damage caused to the data subjects and to third parties, and any other considerations of relevance in determining the degree of illegality and culpability of the specific infringement.
5. If, in the light of the circumstances, there is a qualified diminution of the culpability of the offender or of the illegality of the action, the body applying the penalties shall determine the amount of the penalty by applying the scale for the category of penalties immediately below that for the actual case in question.
6. In no case shall a penalty be imposed which is higher than that laid down in the Law for the category covering the infringement to be punished.
7. The Government shall regularly update the amount of the penalties in accordance with changes in the price indices.

Article 46. *Infringements by public administrations*

1. When the infringements 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 setting out the measures to be adopted to terminate or correct the effects of the infringement. This decision shall be notified to the data controller, the body to which he is responsible, and to the data subjects, if any.
2. The Director of the Agency may also propose that disciplinary proceedings be initiated. The procedure and penalties to be applied shall be those laid down in the legislation on disciplinary proceedings in public administrations.
3. Decisions on the measures and proceedings referred to in the preceding paragraphs shall be communicated to the Agency.
4. The Director of the Agency shall communicate to the Ombudsman the proceedings and decisions taken within the terms of the preceding paragraphs.

Article 47. *Time limits*

1. The time limits for pursuing infringements shall be three years for very serious infringements, two years for serious infringements and one year for minor infringements.
2. The time limits shall start to run on the day on which the infringement was committed,
3. The time limits shall be interrupted when the person concerned is informed of the initiation of the infringement procedure, and the time limit shall recommence if the procedure is held up for more than six months for reasons for which the alleged offender cannot be held responsible.
4. Penalties imposed for very serious infringements shall expire after three years, those imposed for serious infringements after two years, and those imposed for minor infringements after one year.
5. The time limits for penalties shall start to run from the day after the decision imposing the penalty comes into force.
6. The time limits shall be interrupted when the person concerned is informed of the initiation of the execution procedure, and shall recommence if the procedure is held up for more than six months for reasons for which the offender cannot be held responsible.

Article 48. *Penalty procedure*

1. The procedure for determining infringements and imposing the penalties referred to in this Title shall be laid down by regulation.
2. The decisions of the Data Protection Agency or the corresponding body in the Autonomous Community shall exhaust the administrative procedure.

Article 49. *Power to immobilise files*

In cases of very serious infringement, involving the use or illicit transfer of personal data in which the exercise of the rights of citizens and the free development of the personality guaranteed by the Constitution and the laws are seriously impeded or otherwise affected, the Director of the Data Protection Agency may, in addition to imposing a penalty, require the controllers of files personal data in both public and private ownership to terminate the use or illicit transfer of the data. If there is no response to this requirement, the Data Protection Agency may, on the basis of a reasoned decision, immobilise such files for the sole purpose of restoring the rights of the data subjects.

First additional provision. *Existing files*

Files and computer processing operations, whether or not entered in the General Data Protection Register, must comply with this Organic Law within three years of its entry into force. Within this period, files in private ownership must be communicated to the Data Protection Agency, and the public administrations responsible for files in public ownership must approve the relevant provision regulating the files or adapt the existing provision.
In the case of files and data processing operations which are not computerised, compliance with this Organic Law and the obligation in the preceding paragraph must be achieved within twelve years from 24 October 1995, without prejudice to the exercise of the rights of access, rectification and cancellation by the data subjects.

Second additional provision. *Population files and registers of public administrations*

1. Central Government and the administrations of the Autonomous Communities may request from the National Statistical Institute, without the consent of the data subject, an updated copy of the file comprising data on the surname, forenames, domicile, sex and date of birth contained in the municipal censuses of inhabitants and the electoral roll for the territories in which they exercise their powers, for the creation of population files or registers.
2. The purpose of the population files or registers shall be communication between the various bodies in each public administration and data subjects resident in the respective territories, in relation to the legal and administrative relations deriving from the respective remits of the public administrations.

Third additional provision. *Processing of files from the repealed Laws on Vagrants and Malefactors and on Riskiness and Social Rehabilitation*

The files specifically established under the repealed Laws on Vagrants and Malefactors and on Riskiness and Social Rehabilitation, and containing data of whatever sort which might affect the security, reputation, privacy or image of individuals, may not be consulted without the explicit consent of the data subjects or unless fifty years have passed since their date of collection.
In the latter case, the Central Government shall, unless there is proof of the death of the data subjects, make the documentation available to requesters after deleting from it the data referred to in the preceding paragraph using the technical procedures appropriate to each case.

Fourth additional provision. *Amendment to Article 112.4 of the General Law on Taxation*

> "4. The processed personal data which must be transferred to the tax authorities in accordance with the provisions of Article 111, of the preceding paragraphs of this Article, or of other rules of equal standing, shall not require the consent of the data subject. The provisions of paragraph 1 of Article 21 of the Organic Law on Personal Data relating to public administrations shall also not apply to such matters."

Fifth additional provision. *Remit of the Ombudsman and similar regional government bodies*

The provisions of this Organic Law are without prejudice to the remit of the Ombudsman and the similar bodies in the Autonomous Communities.

Sixth additional provision. *Amendment to Article 24.3 on the Law on the Regulation and Supervision of Private Insurances*

Article 24.3, second paragraph, of Law 30/1995 of 8 November, on the Regulation and Supervision of Private Insurances, is amended as follows:

> "Insurance bodies may create joint files containing personal data for the settlement of accident claims and for actuarial statistical collaboration aimed at establishing rates of premiums and the selection of risks, and for drawing up studies on insurance techniques. The transfer of data to such files shall not require the prior consent of the data subject, but the possible transfer of his personal data for the purposes indicated must be communicated to the data subject, together with an explicit indication of the data controller, so that the rights of access, rectification and cancellation laid down by law may be exercised.
> Joint files may also be created without the consent of the data subject for the purpose of preventing insurance fraud. However, it will be necessary in such cases to make known to the data subject, when the data are first introduced, who is responsible for the file and the ways in which the rights of access, rectification and cancellation may be exercised.
> In all cases, data relating to health may be subjected to processing only with the explicit consent of the data subject."

First transitional provision. *Processing operations under international agreements*

The Data Protection Agency shall be the body responsible for the protection of natural persons as regards the processing of personal data, with respect to the processing operations set up under any international agreement to which Spain is a signatory and which assigns this power to a national supervisory authority, unless a different authority is set up for this task in implementation of the agreement.

Second transitional provision. *Use of the publicity register*

The procedures for drawing up the publicity register, for objecting to being entered in it, for making it available to requesters, and for monitoring the lists disseminated, shall be governed by regulation. The regulation shall lay down the time limits for implementation of the publicity register.

Third transitional provision. *Continuation in force of existing rules*

Until such time as the arrangements set out in first final provision of this Law come into force, the existing regulatory rules shall continue in force with their own ranking, and in particular Royal Decrees 428/1993 of 26 March, 1332/1994 of 20 June, and 994/1999 of 11 June, unless they are in conflict with this Law.

Single repealing provision. *Repeal of rules*

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

First final provision. *Authorisation for regulatory development*

The Government shall approve or amend the regulatory provisions necessary for the application and further development of this Law.

Second final provision. *Precepts with the character of ordinary law*

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

Third final provision. *Entry into force*

This Law shall enter into force one month after its publication in the *Boletín Oficial del Estado*.

Therefore
I order all Spaniards, individuals and authorities, to uphold this Organic Law and to ensure that it is upheld.

Madrid, 13 December 1999.

JUAN CARLOS R.

The Prime Minister
JOSÉ MARÍA AZNAR LÓPEZ