Ministerio de Justicia

Constitutional Act 15/1999 on Personal Data Protection

2012

Colección: Traducciones del derecho español

Edita:

Ministerio de Justicia- Secretaría General Técnica

NIPO: 051-12-029-9

Traducción realizada por: Verbatim, S.A

Maquetación: Subdirección General de Documentación y Publicaciones

CONSTITUTIONAL ACT 15/1999 OF 13 DECEMBER ON PERSONAL DATA PROTECTION

Published: Official State Journal No. 298 of 14/12/1999

TITLE I

General provisions

Article 1. Object.

The present constitutional act aims to guarantee and protect the public freedoms and fundamental rights of natural persons, in connection in particular with the processing of their personal data and its impact on the right to protect their honour and their own and their family's privacy.

Article 2. Scope.

1. The present constitutional act shall be applicable to personal data recorded on physical media susceptible to processing, as well as to the subsequent use of these data in whatsoever manner by the public or private sector.

The processing of personal data shall be governed by the present constitutional act:

a) when the data are processed in the context of activities conducted at the controller's establishment, providing such establishment is located on Spanish soil;

b) when the controller is not established on Spanish soil but Spanish legislation is applicable thereto under the terms of international public law;

c) when the controller is not established in the European Union and processes the data with hardware located on Spanish soil, unless such hardware is employed for transit only.

2. The personal data protection provisions laid down in the present constitutional act shall not be applicable to:

a) files kept by natural persons in connection with solely personal or domestic activities;

b) files subject to legislation on the protection of classified information;

c) files created to investigate terrorism and serious organised crime, although in these cases the controller shall notify the Data Protection Agency in advance of the existence of such files, their general characteristics and their purpose.

3. Processing of the following files containing personal data shall be governed by specific legislation or by specific provisions, if any, in this constitutional act:

a) files whose processing and use are governed by electoral legislation;

b) files used exclusively for statistical purposes pursuant to central or regional legislation on public statistics;

c) files whose purpose is to store data contained in the individual classification reports referred to in the legislation on armed forces personnel;

d) files deriving from the Civil Registry and the Central Registry of Convicts and Fugitives;

e) files from video and audio records obtained by law enforcement agencies with video cameras pursuant to the legislation on the subject.

Article 3. Definitions.

For the intents and purposes of the present constitutional act, the terms listed below shall be defined as specified.

a) personal data shall mean any information relating to identified or identifiable natural persons;

b) file shall mean any set of structured personal data, irrespective of the manner in which it is generated, stored, organised or accessed;

c) data processing shall mean operations or procedures, automatic or otherwise, for data collection, recording, storage, formulation, modification, blocking or erasure, as well as the surrender of data deriving from disclosures, queries, interconnections or transfers;

d) controller shall mean the natural or public or private legal person or government body who determines the purpose, content and use of the data processed;

e) data subject shall mean the natural person whose data are processed as referred to in paragraph c) of the present article;

f) decoupling procedure shall mean the processing of personal data in a way that the information obtained cannot be associated with an identified or identifiable person;

g) processor shall mean the natural or legal person, public authority, agency or any other body who, solely or jointly with others, processes personal data on behalf of the controller;

h) data subject's consent shall mean any freely given, specific, unequivocal and informed indication whereby the data subject signifies his agreement to the processing of his personal data;

i) data surrender or disclosure shall mean the act of revealing data to anyone other than the data subject;

j) publicly accessible files shall mean files whose consultation must be open to any individual, unhindered by limiting legislation and contingent upon no other requirement than payment of a fee, as appropriate.

The open census records, telephone listings as provided in the specific legislation in this regard and lists of members of professional associations containing only their name, position, profession, business, academic degree, address and specification of group membership constitute exclusively publicly accessible sources. Daily newspapers, official journals and other media also constitute publicly accessible sources.

TITLE II

Data protection principles

Article 4. Data quality.

1. Personal data may only be collected for processing and processed when they are suited and relevant to and not excessive for the specific, explicit and legitimate scope and purposes for which they were obtained.

2. The personal data processed may not be put to uses incompatible with the purposes for which they were collected. Further processing for historic, statistical or scientific aims shall not be deemed to be incompatible uses.

3. Personal data must be accurate and kept current to ensure that they correctly reflect the data subject's status at all times.

4. If the personal data on record are wholly or partially inaccurate or incomplete, they shall be erased *ex officio* and replaced with the respective rectified or complete data, without prejudice to data subjects' rights as specified in Article 16.

5. Personal data shall be erased when they are no longer necessary or relevant for the purpose for which they were obtained or recorded.

They shall not be stored in a manner in which the data subject can be identified for any longer than necessary for the purposes for which they were obtained or recorded.

Procedures for the exceptional storage of full sets of data deemed to have historical, statistical or scientific value, pursuant to the specific legislation on the matter, shall be laid down in the respective regulations.

6. Personal data shall be stored in a manner that ensures the exercise of the right of access, except where they are legally erased.

7. The use of fraudulent, misleading or illicit means to collect data is prohibited.

Article 5. Right to information during data collection.

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

a) the existence of a personal data file or that the data will be processed, the purpose thereof and the recipients of the information;

b) the obligatory or optional nature of their response to the questions asked;

c) the consequences of providing or refusing to provide the data;

d) the existence of rights of access, rectification, erasure and objection;

e) the identity and address of the controller or, as appropriate, his representative.

When the controller is not established in the European Union but uses data processing hardware located on Spanish soil, he must designate a representative in Spain, unless such hardware is used exclusively for transit purposes. The foregoing is without prejudice to any action that may be brought against the controller himself.

2. When questionnaires or other forms are used to collect the data, they must clearly and legibly specify the cautionary notices referred to in the preceding paragraph.

3. The information specified in sub-paragraphs b), c) and d) of paragraph 1 above shall not be necessary if it can be clearly deduced from the nature of the personal data requested or the circumstances in which they are collected.

4. When personal data are not collected from the data subject, he must be explicitly, precisely and unambiguously informed thereof by the controller or his representative within three months of the date when the data are recorded, unless the data subject was informed in advance of the content to be processed, the source of the data and the information set out in sub-paragraphs a), d) and e) of paragraph 1 of this article.

5. The provisions of the preceding paragraph shall not be applicable when so stipulated explicitly by law; when data are processed for historic, statistical or scientific purposes; when no possibility of informing the data subject exists; or when the Data Protection Agency or equivalent regional body deems that the provision of such information would call for an inordinate effort, account taken of the number of data subjects, the age of the data and possible compensatory measures.

Nor shall the provisions of the preceding paragraph be applicable when the data are extracted from publicly accessible sources and intended for advertising or marketing, in which case all correspondence addressed to the data subject shall include information on the source of the data, the identity of the controller and the rights to which the data subject is entitled.

Article 6. Data subject's consent.

1. The processing of personal data shall be contingent upon the data subject's unambiguous consent thereto, except as otherwise legally provided.

2. Consent shall not be required when the personal data are collected for the purposes of public authorities in the exercise of their competence; when they refer to the parties to an agreement or pre-agreement for a business, employment or administrative relationship and are needed to maintain or perform such agreement; when data are processed to protect the data subject's vital interests under the terms of Article 7, paragraph 6 of the present act; or when the data are contained in publicly accessible sources and their processing is imperative for the purposes of the legitimate interest pursued by the controller or the third party to whom the data are disclosed, providing this entails no violation of the data subject's rights and freedoms.

3. The consent to which the present article refers may be withdrawn for just cause but may not be made retroactive.

4. Where personal data may be processed without the data subject's consent, the data subject may object to the processing of his data on compelling and legitimate grounds relating to his personal situation, except as otherwise legally provided. In such cases, the controller shall refrain from processing the data subject's data.

Article 7. Specially protected data.

1. Further to the provisions of Article 16, paragraph 2 of the Constitution, no one shall be obliged to reveal his ideology, religion or beliefs.

When, in connection with such data, the consent referred to in the following paragraph is requested, the data subject shall be advised of his right not to grant such consent.

2. Personal data that reveal ideology, trade union membership, religion or beliefs may only be processed with the data subject's explicit and written consent. Files kept by political parties, trade unions, churches, faiths or religious communities and associations, foundations and other non-profit–seeking organisations pursuing political, philosophical, religious or trade-union aims shall be excepted as regards the data relating to their members, without prejudice to the requirement of the data subject's prior consent to the surrender thereof.

3. Personal data referring to racial origin, health or sex life may only be collected, processed or transferred when so provided by law for reasons of general interest or where the data subject explicitly grants his consent thereto.

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

5. Personal data relating to the commission of offences or misdemeanours may only be included in the files kept by the competent public authorities in the cases specified 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 required for medical prevention or diagnosis, the provision of health care or medical treatment or health care service management, providing the data are processed by a health care professional bound by professional secrecy or other persons equivalently bound.

The data referred to in the preceding paragraph may also be processed when necessary to safeguard the data subject's or other individual's vital interest, if the data subject is physically or legally unable to grant his consent.

Article 8. Health-related data.

Without prejudice to the provisions on personal data surrender laid down in Article 11, public and private health institutions and centres and the respective professionals may proceed to process personal data relating to the health of the individuals visiting them or treated by them, pursuant to the provisions of central or regional health care legislation.

Article 9. Data security.

1. The controller and, as appropriate, the processor, must adopt all necessary technical and organisational measures to guarantee personal data security and prevent the alteration or loss of, or unauthorised processing of or access to such data, account taken of the state of the art of the technology, the nature of the data stored and the risks to which they are exposed, whether attributable to human action or physical or natural causes.

2. Personal data shall not be recorded in files that fail to meet regulatory requirements respecting their own integrity and security and the integrity and security of processing centres, premises, hardware and software.

3. The requirements and conditions that must be met by the files and individuals involved in processing the data referred to in Article 7 of this act shall be established in the respective regulations.

Article 10. Data secrecy.

The controller and anyone involved in any phase of personal data processing are bound to save such data and to abide by the ethics of professional secrecy in respect thereof. Such obligations shall subsist even after severance of their relationship with the file owner or controller, as appropriate.

Article 11. Data disclosure.

1. Processed personal data may only be disclosed to third parties for purposes directly related to the sender's and the recipient's legitimate activities and providing the data subject lends his prior consent thereto.

2. The consent required by the preceding paragraph shall not be required in the following cases:

a) when surrender is authorised by law;

b) when the data were collected from publicly accessible sources;

c) when the data are processed in connection with a freely accepted legitimate legal relationship whose implementation, performance and control necessarily involve the interconnection between the data processed and third party files.

In the latter case disclosure shall only be legitimate where warranted, i.e., limited to the purpose in question;

d) when the data are to be disclosed to the Ombudsman, the Public Prosecutor, judges or courts or the Court of the Exchequer in the exercise of the duties attributed thereto, or to regional institutions whose duties are analogous to the duties of the Ombudsman or Court of the Exchequer;

e) when surrender involves public authorities and its purpose is further processing for historic, statistical or scientific purposes;

f) when health-related personal data must be surrendered to attend to an emergency that requires accessing a file or to conduct epidemiological studies pursuant to the terms of central or regional health care legislation.

3. Consent to the disclosure of personal data to a third party shall be null and void when the data subject is provided information that fails to reveal the purpose to which the data whose disclosure is authorised will be put or the type of business conducted by the recipient.

4. Consent to personal data disclosure is revocable.

5. Mere disclosure of the personal data itself binds the recipient thereof to observe the provisions of the present act.

6. If the data disclosed are decoupled prior to disclosure, the provisions of the preceding paragraphs shall not be applicable.

Article 12. Third party access to data.

1. Third party access to data shall not be regarded to constitute data disclosure when such access is necessary to provide a service whose recipient is the controller.

2. Third party processing must be regulated in an agreement that must be in written or some other form whereby the conclusion and content thereof can be verified. Such agreement must explicitly specify that the processor may only process the data in accordance with the controller's instructions, that he will not apply them to or use them for any purpose other than laid down in the agreement, nor disclose them to others, even for storage.

The agreement shall likewise stipulate the security measures referred to in Article 9 of this act, which the processor is obliged to implement.

3. After the service defined in the agreement is provided, the personal data must be destroyed or returned to the controller, together with any media or documents containing any personal data processed.

4. If the processor uses the data for any other purpose, discloses them or uses them in breach of the stipulations of the agreement, he shall be regarded to be the controller as well as the processor and be held accountable for any infringements personally committed.

TÍTULO III

Personal rights

Article 13. Right to object to assessments.

1. Citizens are entitled not to be bound by decisions that carry legal or otherwise significant effects based solely on data processing procedures designed to evaluate certain personality or behavioural traits.

2. Data subjects may object to administrative acts or private decisions that entail an assessment of their behaviour based solely on personal data processing that defines their characteristics or personality.

3. In such cases, data subjects shall be entitled to receive information from the controller on the assessment criteria and the software used to adopt the decision on which the action taken was based.

4. Assessments of citizens' behaviour based on data processing shall only hold evidential value when so requested by the data subject.

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

The General Data Protection Registry may be approached by anyone wishing to obtain information on the existence of files containing their personal data, the purpose of such files or the identity of the controller. The information in the General Registry shall be public and cost-free.

Article 15. Right of access.

1. Data subjects shall be entitled to request and obtain, at no cost whatsoever, information on the personal data processed by the controller, the origin of such data and any past or intended future disclosure thereof.

2. Such information may be obtained in response to an inquiry by simple visualisation of the data, or in writing, in which the data being processed shall be described on a legible and comprehensible copy, telecopy or photocopy, certified or otherwise. Such information shall contain no codes whose interpretation calls for specific hardware.

3. The right to access referred to in this article may be exercised at no less than twelve-month intervals, except where the data subject accredits a legitimate interest, in which case it may be exercised earlier.

Article 16. Rights of rectification and erasure.

1. The controller shall be obliged to rectify or erase the data subject's personal data within ten days of the exercise of the respective rights by the latter.

2. Personal data shall be rectified or erased when processed in a manner that fails to comply with the provisions of the present act and in particular when such data are inaccurate or incomplete.

3. Data erased shall be blocked and thereafter may be saved solely for the use of public authorities, judges and courts to attend to possible liabilities deriving from their processing, and only for as long as such liability is claimable.

The data shall be deleted when the period of liability lapses.

4. Where the data rectified or erased were disclosed prior to rectification or erasure, the controller must notify the data recipient thereof, who must also proceed to erase the data if processing is still underway.

5. Personal data must be kept for the length of time provided in the applicable legislation or, as appropriate, in the agreements between the controller and the data subject.

Article 17. Objection, access, rectification and erasure procedures.

1. The procedures for exercising the right to object, access, rectify and erase shall be established in the respective regulations.

2. No consideration whatsoever shall be demanded for exercising the rights of objection, access, rectification or erasure.

Article 18. Legal protection of rights.

1. Conduct contrary to the provisions of the present act may be reported by the data subject to the Data Protection Agency in the manner specified in the respective regulations.

2. Data subjects who are wholly or partially denied the exercise of their rights of objection, access, rectification or erasure may notify the Data Protection Agency or, as appropriate, the competent regional authority, accordingly. It shall be incumbent upon the agency or the competent authority to ascertain whether such denial is rightful or otherwise.

3. An explicit resolution on the protection of such rights shall be issued within no more than six months.

4. The resolutions delivered by the Data Protection Agency may be appealed via judicial review.

Article 19. Right to indemnity.

1. Where controllers' or processors' failure to comply with the provisions of the present act is detrimental to data subjects' property or rights, the parties concerned shall be entitled to indemnity.

2. In the event of public sector files, liability claims shall be lodged and handled as specified in the legislation on Government liability.

3. In the event of private sector files, liability action shall be brought before ordinary judiciary bodies.

TITLE IV

Sectoral provisions

CHAPTER I

Public sector files

Article 20. Creation, modification or deletion.

1. Public authorities may only create, modify or delete files when a general provision is adopted in this regard and published in the *Official State Journal* or analogous regional publication.

2. Provisions creating or modifying files shall specify the following:

a) the purpose of the file and the envisaged use;

b) the persons or groups whose personal data are to be gathered or who are obliged to furnish such data;

c) the procedure for gathering the personal data;

d) the basic structure of the file and description of the types of personal data included therein;

e) any surrender of personal data and, as appropriate, any planned transfer of data to third countries;

f) the public bodies responsible for the file;

g) the services or units that may be addressed to exercise the rights of access, rectification, erasure and objection;

h) specification of whether the file is subject to low, medium or high level security.

3. The provisions decreed to delete files shall specify the destination thereof or, as appropriate, the measures to be adopted for their destruction.

Article 21. Data disclosure between public authorities.

1. The personal data gathered or compiled by public authorities in the performance of their duties may not be disclosed to other public authorities to perform duties of a different nature or relating to different matters, except *where provision was made therefor in the legislation creating the file or by higher ranking legislation regulating its use*, or when the data are disclosed for subsequent processing for historical, statistical or scientific purposes.

2. When personal data are obtained or compiled by one public authority for another, they may always be disclosed to the intended recipient.

3. Notwithstanding the provisions of Article 11.2.b), data gathered from publicly accessible sources may not be disclosed to private sector files except where the law allows or the data subject consents thereto.

4. In the cases envisaged in paragraphs 1 and 2 of the present article, the data subject's consent provided for in Article 11 of the present act shall not be required.

Article 22. Files kept by law enforcement bodies.

1. Files created by law enforcement bodies containing personal data that, having been gathered for administrative purposes, must be kept on permanent record, shall be subject to the general provisions of the present act.

2. Personal data gathering and processing for law enforcement purposes by the police force or corps without the consent of the data subjects shall be limited to the cases and data categories required to prevent objective risks to public safety or to repress offences, and such data must be stored in specific files established for this purpose and categorised by their degree of reliability.

3. The data referred to in paragraphs 2 and 3 of Article 7 may be gathered and processed by law enforcement agencies only where absolutely necessary for the purposes of a specific investigation, without prejudice to control of the legality of the administrative action or to the obligation of the judiciary bodies to deliver resolutions on claims lodged by the data subjects.

4. Personal data recorded for law enforcement purposes shall be erased when no longer required for the inquiry that occasioned their storage.

To this end, particular consideration shall be given to the age of the data subject, the nature of the data stored, the need to keep the data through conclusion of a specific investigation or proceeding and the final verdict, especially in the event of acquittal, pardon, rehabilitation or extinguishment of liability.

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

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 erasure, in view of the risk such action might entail for State security or public safety, the protection of third party rights and freedoms or the needs in connection with investigations underway.

2. Treasury file controllers may likewise deny the exercise of the rights referred to in the preceding paragraph when consent thereto might obstruct administrative action tending to ensure compliance with tax obligations and, regardless of any other consideration, when the data subject is being audited.

3. The denial, in whole or in part, of the exercise of the rights mentioned in the preceding paragraphs may be reported to the Director of the Data Protection Agency or, where the files involved are kept by the respective regional police force or regional tax authority, the competent regional body. In whichever case, the data protection body must ascertain whether such denial is rightful or otherwise.

Article 24. Other exceptions to data subjects' rights.

1. The provisions of paragraphs 1 and 2 of Article 5 shall not be applicable to data collection when informing the data subject *constitutes a severe hindrance or impediment to the public authorities' compliance with their supervisory and verification duties* or when national defence, public safety or the persecution of offences or *misdemeanours* are involved.

2. (Cancelled).

CHAPTER II

Private sector files

Article 25. Creation.

Private sector personal data files may be created when necessary for the individual's, company's or entity's legitimate activity or objective, providing the guarantees laid down in the act for personal protection are honoured.

Article 26. Notification and entry in the registry.

1. Any individual or entity in the process of creating a personal data file shall notify the Data Protection Agency in advance thereof.

2. Regulations shall be enacted for the detailed description of the items to be covered in the notification, which shall necessarily include the controller, the purpose, the location, the type of personal data contained, the security measures, specifying whether low, medium or high level security is required, and any surrender of personal data or, as appropriate, any planned international transfer of personal data to third countries.

3. The Data Protection Agency must be notified of the changes in the purpose or location of the automatic file or in the identity of the controller.

4. The General Data Protection Registry shall enter the file if the notification meets the applicable requirements.

Otherwise, it may request that the missing or erroneous data be furnished or rectified.

5. If the Data Protection Agency fails to deliver a resolution within one month of the submission of the application for registration, the automatic file shall be understood to be entered for all intents and purposes.

Article 27. Notification of data surrender.

1. On the occasion of the first data surrender, the controller must inform the data subjects thereof, also specifying the purpose of the file, the nature of the data surrendered and the name of the recipient.

2. The obligation laid down in the preceding paragraph shall not be applicable to the cases envisaged in Article 11, paragraphs 3, sub-paragraphs c), d), e), and 6, nor when surrender is legally mandated.

Article 28. Data in publicly accessible sources.

1. The personal data contained in the open census records or lists of persons pertaining to the professional associations referred to in Article 3, j) of the present act must be limited to the information strictly necessary to fulfil the purpose of each listing. The inclusion of additional data by the controllers responsible for maintaining such sources shall be contingent upon the data subject's consent, which may be revoked at any time.

2. Data subjects shall be entitled to require the controller responsible for maintaining the lists of members of professional chartered institutions to specify, at no cost to the data subjects, that their personal data may not be used for advertising or marketing purposes.

Data subjects shall be entitled to require the exclusion, cost-free, of all their personal data from the open census records by the controllers in charge of maintaining such sources.

Requests for exclusion of unnecessary information or the inclusion of the objection to the use of data for advertising or distance selling must be attended to within ten days for information retrieved telematically and in the subsequent edition of the listing, regardless of the medium in which they are published.

3. Publicly accessible sources published in book form or any other hard copy format shall lose their publicly accessible status when the following edition is released.

Where a copy of the listing is obtained in electronic format via telematic methods, it shall retain its status as a publicly accessible source for only one year counting from the date it was obtained.

4. The data contained in publicly accessible telecommunication service listings shall be governed by specific legislation.

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

1. Parties engaging in the provision of information on solvency and creditworthiness may only process personal data when obtained from publicly accessible records and sources established for this purpose or from information provided by or with the consent of the data subject.

2. They may also process personal data relating to the compliance or non-compliance with financial obligations furnished by the creditor or party acting in the creditor's name or on his behalf. In such cases the data subjects whose personal data are recorded in files shall be notified of the data included in the file within thirty days of the date the information is recorded. They shall likewise be informed of their right to obtain information on all such data under the terms of the present act.

3. In the cases referred to in the two preceding paragraphs, when the data subject so requests, he shall be notified by the controller of the data involved, the assessments and appraisals referring thereto received in the last six months, and the name and address of the individual or entity to whom such data were disclosed.

4. Only personal data that are decisive for judging data subjects' financial solvency may be recorded and surrendered, and when adverse, the historical series may cover no more than six years, and only when they provide a true view of the data subjects' current financial situation.

Article 30. Data processed for advertising and marketing purposes.

1. Persons engaging in compiling addresses, distributing documents, advertising, distance selling, marketing or similar activities may use names and addresses and other personal data when these data are contained in publicly accessible sources or are furnished by the data subjects or obtained with their consent.

2. When the data are drawn from publicly accessible sources pursuant to sub-paragraph two of Article 5.5 of this act, all correspondence addressed to the data subject shall specify the origin of the data and identity of the controller, as well as the rights to which the former is entitled.

3. In exercising their right of access, data subjects shall be entitled to be informed of the origin of their personal data and the rest of the particulars listed in Article 15.

4. Data subjects shall be entitled to object, via cost-free request, to the processing of their data, in which case the information referring thereto shall be erased in response to such request.

Article 31. Open census records.

1. Persons engaging continuously or sporadically in compiling addresses, distributing documents, advertising, distance selling, marketing or similar activities may ask the National Statistics Institute or equivalent regional bodies to furnish them with a copy of the open census records, showing the names, surnames and addresses contained in the electoral census.

2. Each set of open census records may be used validly for one year. Once that period has lapsed, the records shall no longer be regarded to be a publicly accessible source.

3. The procedures whereby data subjects may request to be excluded from the open census records shall be established in the respective regulations. These procedures, which shall be cost-free for data subjects, shall include the certificate of registration in the municipal census.

A current listing of the open census records shall be published quarterly, excluding the names and addresses of the parties requesting exclusion.

4. Consideration may be required for provision of the listing on electronic media.

Article 32. Standard codes.

1. Public and private controllers and the organisations under which they are grouped may formulate standard codes further to sectoral or government body agreements or company decisions. Such codes may establish recommendations for organisation; operating schemes; applicable procedures; security rules for premises, hardware or software; obligations of the persons involved in processing; use of personal information; and guarantees, in the respective scope, for the exercise of personal rights. All these recommendations must conform to the principles and provisions of the present act and any regulations relating thereto.

2. The aforementioned codes may contain detailed operating rules for each specific system and technical standards for their application.

Where no such rules or standards are explicitly included in the code, the instructions or orders whereby they are established must honour the principles laid down therein.

3. Standard codes shall be regarded to be codes of conduct or good professional practice and must be deposited with or entered in the General Data Protection Registry and, as appropriate, in the registries created for this purpose by the Autonomous Communities further to Article 41. The General Data Protection Registry may deny such entry when the codes fail to comply with the legal and regulatory provisions on the subject, in which case the Director of the Data Protection Agency shall require the applicants to amend them accordingly.

TITLE V

International data transfers

Article 33. General rule.

1. Personal data that have been processed or collected for processing may not be temporarily or permanently transferred to countries that fail to provide a level of protection comparable to the protection afforded by the present act unless, in addition to compliance with the provisions hereunder, prior authorisation is secured from the Director of the Data Protection Agency. Authorisation may only be granted where sufficient guarantees are furnished.

2. The suitability or otherwise of the level of protection afforded by the recipient country shall be evaluated by the Data Protection Agency on the grounds of all the circumstances surrounding the data transfer or data transfer category. More specifically, account shall be taken of the nature of the data, purpose and duration of the processing operation or planned processing operations, the countries of origin and final destination, the general or sectoral legal provisions in place in the third country in question, the content of the European Commission's reports and the professional provisions and security measures in effect in such countries.

Article 34. Exceptions.

The provisions of the preceding article shall not be applicable in the following circumstances:

a) when the international transfer of personal data stems from the application of treaties or conventions to which Spain is a party;

b) when the data are transferred to provide or request international judicial support;

c) when the transfer is necessary for medical prevention and diagnosis, the provision of health care or medical treatments, or health care service management;

d) when the data involved relate to transfers of funds in accordance with the specific legislation in that regard;

e) when the data subject has unequivocally consented to the planned transfer;

f) when the transfer is necessary for the performance of a contract between the data subject and the controller or to adopt pre-contractual measures taken at the data subject's request;

g) when the transfer is necessary for the execution or performance of a contract concluded or to be concluded, in the data subject's interest, between the controller and a third party;

h) when the transfer is necessary or legally required to safeguard the public interest;

   this shall include transfers requested by a tax or customs authority in the exercise of its duties;

i) when the transfer is necessary for the acknowledgement, exercise or defence of a right in court proceedings;

j) when the transfer is effected from a public registry at the request of an individual with a legitimate interest and is in keeping with the purpose of the former;

k) when the destination of the transfer is a European Union Member State or a state which, pursuant to an appraisal issued by the Commission of the European Communities in the exercise of its duties, provides an adequate level of protection.

TITLE VI

Data Protection Agency

Article 35. Nature and legal status.

1. The Data Protection Agency, a public body acting independently of governmental authority, has a legal personality of its own and full legal capacity for private and public actions. It shall be governed by the provisions of the present act and its own by-laws, which must be approved by the Government.

2. In the exercise of its public duties and for matters not addressed in the present act or the regulations relating thereto, the Data Protection Agency shall be governed in accordance with Act 30/1992 of 26 November on the Legal Framework for Public Authorities and General Administrative Procedures. Its acquisition of assets and hiring shall be subject to private law.

3. Positions with the bodies and services comprising the Data Protection Agency shall be filled by public officials or specifically hired staff, depending on the nature of the duties assigned to each position. All personnel shall be bound by professional secrecy in respect of the personal data to which they have access in the exercise of their duties.

4. The Data Protection Agency shall be provided with the following ways and means to fulfil its purpose:

a) the yearly allocations established in the National Budget;

b) property or securities in its possession, and any returns thereon;

c) any others that may be lawfully attributed thereto.

5. The Data Protection Agency shall formulate and approve its yearly preliminary draft budget and submit it to the Government for its inclusion, with all due independence, in the National Budget.

Article 36. The Director.

1. The Director of the Data Protection Agency manages and represents the Agency. He shall be designated by Royal Decree for a four-year term from among the members of the Advisory Board.

2. The Director shall perform his duties independently and objectively and shall be subject to no manner of instructions whatsoever in the performance thereof.

In any event, the Director shall systematically hear the proposals put forward by the Advisory Board in the exercise of its duties.

3. The Director of the Data Protection Agency may be separated from office prior to expiration of the term referred to in paragraph 1 only upon his own request or if dismissed by the Government. Such dismissal shall be subject to the institution of proceedings, in which the other members of the Advisory Board must necessarily be heard, for gross dereliction of duties, onset of the incapacity to perform the duties required of the position, incompatibility or conviction for a wilful offence.

4. The Director of the Data Protection Agency shall have senior executive status and, if he had formerly been in public service, he shall be engaged under secondment arrangements. If the Director designated is a member of the judiciary or the prosecution service, he shall likewise be engaged under secondment arrangements.

Article 37. Duties.

1. The Data Protection Agency Director's duties include the following:

a) enforcing data protection legislation and monitoring its application, in particular as regards the rights of information on, access to, rectification of, objection to and erasure of data;

b) issuing the authorisations provided for in this act or related regulations;

c) delivering instructions for the adjustment of data processing to the principles laid down in this act, as appropriate and without prejudice to the competencies of other bodies;

d) handling the requests and claims lodged by data subjects;

e) furnishing information on rights in respect of personal data processing;

f) requiring data processing controllers and processors, after hearing their allegations, to adopt the necessary measures to adapt their data processing systems to the provisions of this act and, as appropriate, ordering erasure and discontinuation of the processing of files that fail to comply with such provisions;

g) exercising power to impose penalties under the terms laid down in Title VII of this act;

h) issuing a mandatory report on the draft general provisions relating to this act;

i) obtaining from controllers any assistance or information deemed necessary for the performance of his duties;

j) ensuring the public disclosure of the existence of personal data files, to which end a list of the files on record shall be published from time to time, together with any additional information specified by the Director of the Agency;

k) drafting an annual report for submission to the Ministry of Justice;

l) monitoring international data transfers, issuing any authorisations that may be in order in connection therewith and performing any duties relating to international cooperation on personal data protection;

m) ensuring compliance with the provisions laid down in the Act on Public Statistics on the gathering of statistical data and statistical secrecy, and issuing any necessary instructions in that regard, establishing the security conditions to be met by files developed exclusively for statistical purposes and exercising the powers vested in him under Article 46;

n) any other duties legally attributed thereto;

2. The resolutions delivered by the Spanish Data Protection Agency shall be made public, preferably via information and communication technology methods, after notice thereof is served upon the parties concerned.

The terms whereby such public disclosure shall be conducted may be established in the respective regulations.

The provisions set out in the foregoing shall not be applicable to resolutions relating to the entry of a file or processing system in the General Data Protection Registry or to the registration of the standard codes regulated under Article 32 of the present constitutional act.

Article 38. Advisory Board.

The Director of the Data Protection Agency shall be counselled by an Advisory Board whose membership shall include:

one member of Parliament nominated by the Congress of Deputies;

one senator nominated by the Senate;

one representative of the Central Government nominated by the Government;

one local government representative nominated by the Spanish Federation of Municipalities and Provinces;

one member of the Royal Academy of History nominated by the said academy;

one expert in the area nominated by the Senior Council of Universities;

one member representing users and consumers, selected as stipulated in the respective regulations;

one representative of each autonomous community that has created a regional data protection agency, nominated pursuant to the procedure established by the respective autonomous community;

one representative of the private personal data processing industry, to be nominated pursuant to the procedure laid down in the respective regulations.

The Advisory Board's *modus operandi* shall be governed by the regulations enacted to that end.

Article 39. The General Data Protection Registry.

1. The General Data Protection Registry is a body under the aegis of the Data Protection Agency.

2. The following shall be entered in the General Data Protection Registry:

a) public sector files;

b) private sector files;

c) the authorisations provided for in the present act;

d) the standard codes referred to in Article 32 of the present act;

e) all data on files required to enable data subjects to exercise their rights of information, access, rectification, erasure and objection.

3. Procedures shall be laid down in the respective regulations, for both private and public sector files, for: file entry in the General Data Protection Registry, entry content, amendment, erasure, claims and appeals challenging the respective resolutions, and all other pertinent items.

Article 40. Power of inspection.

1. Supervisory authorities may inspect the files referred to in the present act, obtaining whatsoever information may be needed to fulfil their duties.

To this end, they may ask for documents to be displayed or furnished or proceed to their examination wherever they are custodied, and access the premises where the hardware and software used for data processing are installed for the purposes of inspection.

2. Officials who conduct the inspections referred to in the preceding paragraph shall be vested with public authority status in the performance of their duties.

They shall be bound by professional secrecy respecting the information accessed in the exercise of such duties, even after discontinuation thereof.

Article 41. Respective regional bodies.

1. The Data Protection Agency's duties laid down in Article 37, excepting paragraph 1, sub-paragraphs j), k) and l), and sub-paragraphs f) and g) regarding international data transfers, as well as in Articles 46 and 49 respecting its specific competencies, shall be performed by the respective regional bodies when the personal data files involved are created or managed by autonomous communities or local governments within their respective

territorial limits. Such bodies shall be vested with enforcement authority status and perform their duties independently and objectively.

2. The Autonomous Communities may create and maintain their own data records for the exercise of the competencies acknowledged thereto.

3. The Director of the Data Protection Agency may routinely convene meetings of the respective regional bodies for the intents and purposes of institutional cooperation and coordination of criteria or procedures for action. The Director of the Data Protection Agency and respective regional bodies may request information from one another where required to perform their duties.

Article 42. Autonomous Community files respecting areas of their exclusive competence.

1. When the Director of the Data Protection Agency becomes aware that the maintenance or use of a given file in an Autonomous Community infringes any of the provisions of this act in an area of the exclusive competence of the latter, he may determine the necessary corrective measures and require their adoption by the respective authority within a deadline explicitly stated in the notice.

2. If the respective public authority fails to comply with the requirement formulated, the Director of the Data Protection Agency may challenge the resolution delivered by the said authority.

TITLE VII

Infringements and penalties

Article 43. Controllers and processors[1].

1. Controllers and processors shall be subject to the system of penalties laid down in the present act.

2. For files in the possession of public authorities, the procedures and penalties shall be as provided in Articles 46 and 48 of the present act.

Article 44. Types of infringements[2].

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

2. The infringements listed below are minor:

a) failure to furnish the Spanish Data Protection Agency with the information laid down in this act or related regulatory provisions;

b) failure to apply for registration of personal data files with the General Data Protection Registry;

c) failure to comply with the duty to inform data subjects that their personal data will be processed when these data are obtained from the subjects themselves;

d) data transfer to a processor without completing the formalities laid down in Article 12 of this act;

3. The infringements listed below are serious:

a) creating public sector files or initiating personal data collection for such files without due authorisation under the terms of a general provision published in the Official State Journal or respective official regional journal;

b) processing personal data without obtaining the data subjects' consent where such consent is mandatory pursuant to this act and related regulatory provisions;

c) processing or subsequently using personal data in breach of the principles and guarantees established in Article 4 of this act or in any related regulatory provisions, when this dos not constitute a very serious infringement;

d) failing to comply with the secrecy obligations in connection with personal data processing laid down in Article 10 of this act;

e) hindering or obstructing the exercise of the rights of access, rectification, erasure or objection;

f) failing to comply with the duty to inform data subjects that their personal data will be processed when these data are not obtained from the subjects themselves;

g) failing to comply with the remaining obligations in connection with notifying data subjects or requesting their consent as laid down in this act or related regulatory provisions;

h) maintaining files, physical premises, software or hardware containing personal data that fail to meet the security requirements laid down in the respective regulations;

---

[1] Paragraph 2 amended by final provision 56.1, Act 2/2011 of 4 March

[2] Paragraphs 2 to 4 amended by final provision 56.2, Act 2/2011 of 4 March

i) failing to fulfil Spanish Data Protection Agency requests, heed its admonitions or furnish it with the documents or information requested thereby;

j) obstructing inspection activities;

k) disclosing or surrendering personal data without lawful entitlement to do so under the provisions of this act or related regulatory provisions, when this does not constitute a very serious infringement.

4. The infringements listed below are very serious:

a) engaging in misleading and fraudulent data collection;

b) processing or surrendering the personal data referred to in Article 7, paragraphs 2, 3 and 5 of this act, except where authorised thereby, or violating the prohibition contained in Article 7, paragraph 4;

c) failing to desist in the unlawful processing of personal data when formally required to do so by the Director of the Spanish Data Protection Agency;

d) transferring personal data abroad to countries that do not ensure a comparable level of protection without authorisation from the Director of the Spanish Data Protection Agency, except where such authorisation is not required hereunder or in any related regulatory provisions.

Article 45. Type of penalties[3].

1. Minor infringements shall be punished with a fine of from 900 to 40 000 euros.

2. Serious infringements shall be punished with a fine of from 40 001 to 300 000 euros.

3. Very serious infringements shall be punished with a fine of from 300 001 to 600 000 euros.

4. The amount of the fines shall be determined further to the following criteria:

a) persistence in committing the infringement;

b) the volume of data involved;

c) the relationship between the transgressor's activity and the processing of personal data;

d) the transgressor's turnover;

e) the profits obtained by committing the infringement;

f) the degree of intentionality;

g) the recurrent commission of infringements of the same nature;

h) the nature of the damage caused to the data subjects or third parties;

i) substantiation that prior to the events constituting the infringement, the entity accused had suitable personal data collection and processing procedures in place and that the infringement was due to the anomalous performance of such procedures and not to a lack of diligence for which the transgressor could be held liable;

j) any other circumstance relevant to determining the degree of unlawfulness or culpability involved in the infringement in question.

5. The authority imposing the penalty may establish the amount of the fine on the basis of the scale for the class of infringements immediately less serious than the class corresponding to the infringement in question in the following circumstances:

[3] Paragraphs 1 to 5 amended, paragraphs 6 and 7 renumbered as 7 and 8 and paragraph 6 added, pursuant to final provision 56.3 and 4, Act 2/2011 of 4 March.

a) when the culpability of the accused or the unlawfulness of the deed is perceived to be of lesser essence as a result of the existence, in significant measure, of several of the criteria listed in paragraph 4 of this article;

b) when the transgressor diligently rectifies the irregular situation;

c) when the data subject's behaviour can be perceived to have induced the commission of the infringement;

d) when the transgressor spontaneously acknowledges culpability;

e) in the event of takeovers, when the infringement is prior to that process and not attributable to the acquiring company.

6. Exceptionally, after hearing the parties concerned and considering the nature of the deeds and the existence, in significant measure, of the criteria laid down in the preceding paragraph, the authority imposing the fine may abstain from instituting penalty proceedings. It may instead admonish the controlling entity to substantiate the adoption of pertinent corrective measures within the deadline established by the authority, providing the following conditions are met:

a) the deeds constitute a minor or serious infringement pursuant to the provisions hereunder;

b) the transgressor has not been previously fined or admonished.

If the admonishment is not heeded within the deadline set by the authority imposing the fine, institution of the respective penalisation proceedings shall be in order.

7. Fines higher than the highest amount stipulated in this act for the infringement penalised may not be imposed under any circumstances.

8. The Government shall update the amounts of the fines on a regular basis in accordance with the variations in price indices.

Article 46. Infringements by public authorities[4].

1. When the infringements referred to in Article 44 involve files in the possession of public authorities or processing conducted by controllers who are public officials, the authority imposing the fine shall deliver a resolution establishing the measures to be adopted to halt the infringements or correct the effects thereof. Notice of this resolution shall be served upon the controller, the body under whose aegis he operates and the data subjects, if any.

2. The authority imposing the fine may also propose the institution of disciplinary action, if in order. The procedures and penalties to be applied shall be as stipulated in the legislation on disciplinary action for public authorities.

3. The authority imposing the fine shall be notified of the resolutions resulting from the measures and actions referred to in the preceding paragraphs.

4. The Director of the Agency shall notify the Ombudsman of the actions taken and the resolutions delivered pursuant to the preceding paragraphs.

Article 47. Extinguishment.

1. The period during which prosecution may be brought for very serious infringements shall be three years, for serious infringements two and for minor infringements one.

2. The aforementioned terms shall be counted from the time the infringement was committed.

[4] Paragraphs 1 to 3 amended by final provision 56.5, Act 2/2011 of 4 March

3. Such terms shall be interrupted upon institution of penalisation proceedings and notification of the party concerned thereof, but resumed if the proceedings are suspended for over six months for reasons not attributable to the alleged infringer.

4. Fines imposed for very serious misdemeanours shall lapse after three years, for serious misdemeanours after two and for minor misdemeanours after one.

5. The aforementioned terms shall be counted from the day following the day on which the final resolution imposing the fine is issued.

6. Such terms shall be interrupted with the institution of enforcement proceedings, of which the party concerned shall be duly informed, but shall be resumed if such proceedings are suspended for over six months for reasons not attributable to the infringer.

Article 48. Penalisation procedure.

1. The procedure for determining infringements and imposing the fines referred to in the present title shall be established in the respective regulations.

2. Resolutions delivered by the Data Protection Agency or analogous regional body shall not be subject to judicial review.

3. The maximum duration of the penalisation proceedings handled by the Spanish Data Protection Agency in the exercise of the competencies attributed thereto by this or other laws, with the exception of infringements of General Telecommunications Act 32/2003 of 3 November, shall be six months.

Article 49. Power to immobilise files[5].

In cases of serious or very serious infringements in which the persistent processing, international disclosure or transfer of personal data may constitute a serious attempt against citizens' fundamental rights and in particular their right to personal data protection, the authority imposing the fine may, in addition to exercising its power to impose penalties, require the private or public sector controllers of personal data files to discontinue their illegal use or surrender of the data in question. If such notice goes unheeded, the authority imposing the fine may, subject to a duly justified resolution, immobilise such files for the sole purpose of restoring data subjects' rights.

[5] Amended by final provision 56.6 of Act 2/2011 of 4 March

Additional provision one. Pre-existing files.

Presently existing files and their automatic processing, registered or otherwise with the General Data Protection Registry, shall be adapted to the provisions of the present constitutional act within no more than three years, counting from the date of the entry into effect of the act.

The Data Protection Agency must be notified of private sector files within that term and the controllers of public sector files must approve provisions regulating the files in question or adapt any existing provisions accordingly.

Non-automatic files and processing methods must be adapted to the provisions of the present constitutional act and the obligation set out in the preceding paragraph must be met within twelve years counting from 24 October 1995, without prejudice to data subjects' rights of access, rectification and erasure.

Additional provision two. Public authorities' population files and records.

1. The Central and Regional Governments may ask the National Statistics Institute, with no need to obtain data subjects' consent, for an updated copy of the file containing the first and last names, address, sex and date of birth recorded in the municipal and electoral censuses for the regions of their competence, to create population files or records.

2. The purpose of population files or records shall be to enable the bodies under the aegis of each public authority to correspond with data subjects residing in their respective regions in connection with the legal and administrative relations deriving from public authorities' respective competencies.

Additional provision three. Processing of the proceedings under the repealed Loiterers and Rogues and Social Hazard and Rehabilitation Acts.

Proceedings instituted specifically under the Loiterers and Rogues or Social Hazard and Rehabilitation Acts, now repealed, and containing data of whatsoever nature liable to affect data subjects' safety, honour, privacy or personal image may not be consulted unless explicitly consented to by the data subjects or unless fifty years have lapsed since institution of the proceedings.

In the latter event, barring explicit knowledge of the decease of the data subjects involved, the Central Government shall provide the applicant with the documents, from which the data alluded to in the preceding paragraph shall be deleted via the most suitable technical procedures in each case.

Additional provision four. Amendment of Article 112.4 of the General Taxation Act.

Article 112, paragraph 4 of the General Taxation Act shall be reworded as shown below.

"4. The data subject's consent shall not be required for the surrender of personal data to the tax authority for processing in accordance with the provisions of Article 111, the preceding paragraphs of this article or any other provisions with the status of law.

"Nor shall the provisions of Article 21, paragraph 1 of the Constitutional Act on Personal Data Protection be applicable to the public authorities in this domain."

Additional provision five. Competencies of the Ombudsman and similar regional bodies.

The provisions of the present constitutional act are understood to be without prejudice to the competencies reserved to the Ombudsman and analogous regional bodies.

Additional provision six. Amendment of Article 24.3 of the Act on the Regulation and Supervision of Private Insurance.

The second sub-paragraph of Article 24.3 of Act 30/1995 of 8 November on the Regulation and Supervision of Private Insurance is amended to read as shown below:

"Insurers may establish collective files containing personal data for the purposes of claim settlement, compilation of actuarial statistics to value and select risks, and conduct studies on insurance techniques.

The transfer of data to such files shall not be subject to the prior consent of the data subjects, who must, however, be informed of the possible surrender of their personal data to such collective files for the purposes specified. These notices must explicitly indicate the identity of the controller to enable data subjects to exercise their rights of access, rectification and erasure provided by law.

”Collective files may also be established to prevent insurance fraud, for which the consent of the data subject shall not be necessary. When their data are entered for the first time, however, data subjects must be notified of the identity of the file controller and the manners in which they may exercise their rights of access, rectification and erasure.

”Health-related data may only be processed where consented to by the data subject.”

Transitional provision one. Files created by international conventions.

The Data Protection Agency shall be the competent authority in charge of protecting natural persons with respect to the processing of their personal data further to any international convention to which Spain is party, where such competence is attributed to a national supervisory authority, until such time as another authority is created for that purpose under the convention.

Transitional provision two. Use of open census records.

The procedures for generating open census records, objecting to appearance therein, provision thereof on request and monitoring the lists distributed shall be established in the respective regulations.

Such regulations shall also establish the terms within which open census records must be established.

Transitional provision three. Subsistence of pre-existing rules.

Until such time as the terms of the first final provision of this act materialise, the existing regulations, in particular Royal Decrees 428/1993 of 26 March, 1332/1994 of 20 June and 994/1999 of 11 June, shall remain in force with their present status, except where they may conflict with the provisions of the present act.

Sole repealing provision. Repeal of legislation.

Constitutional Act 5/1992 of 29 October on the Regulation of the automatic processing of personal data is hereby repealed.

Final provision one. Authorisation to establish regulations.

The Government shall approve or amend the regulatory provisions necessary to apply the present act.

Final provision two. Ordinary law status.

Titles IV, VI except the final mention in Article 36, paragraph 4, and VII of the present act, as well as additional provision four, transitional provision one and final provision one, constitute legislation with the status of ordinary law.

Final provision three. Entry into force.

The present act shall enter into force one month after its publication in the *Official State Journal*.