Ministerio de Justicia

Royal Decree 1720/2007 relating to 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

ROYAL DECREE 1720/2007 OF 21 DECEMBER APPROVING THE REGULATIONS RELATING TO CONSTITUTIONAL ACT 15/1999 OF 13 DECEMBER ON PERSONAL DATA PROTECTION

Official State Journal No. 17 of 19/01/2008

Constitutional Act 15/1999 of 13 December on Personal Data Protection adapted our laws to the provisions of European Parliament and Council Directive 95/46/EC of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data and repealed Constitutional Act 5/1992 of 29 October on the Regulation of the Automatic Processing of Personal Data, which had been in force until that time.

The new act, drafted in very general terms, provides in Article 1 that it "aims to guarantee and protect the public freedoms and fundamental rights of natural persons, in particular the right to protect their honour and their own and their family's privacy, with respect to the processing of their personal data." Consequently, it covers both the automatic and non-automatic processing of personal data.

In order to guarantee the necessary legal certainty in such a sensitive domain of fundamental rights as data protection, the legislator confirmed the validity of the existing regulations, in particular Royal Decrees 428/1993 of 26 March, Approving the Data Protection Agency By-laws, 1332/1994 of 20 June Relating to Certain Provisions in Constitutional Act 5/1992 of 29 October on the Regulation of the Automatic Processing of Personal Data and 994/1999 of 11 June Approving the Regulations on Security Measures for Automatic Files Containing Personal Data. At the same time, the Government was empowered to approve or amend regulatory provisions as necessary to apply and elaborate on Constitutional Act 15/1999.

Moreover, Act 34/2002 of 11 July on Information Society and Electronic Commerce Services and General Act 32/2003 of 3 November on Telecommunications vest the Spanish Data Protection Agency with competence to impose penalties. Such competence calls for the establishment of regulatory provisions, with the particularity that both legal texts address the rights not only of natural but also of legal persons.

II

These regulations share with the constitutional act the aim of confronting the risks for privacy rights that may be entailed in the stockpiling and processing of personal data. In this regard, the present provisions are designed not to reiterate the content of the higher-ranking legislation but to regulate, not only the mandates set out in the constitutional act pursuant to the principles laid down in the directive, but also the questions requiring more detailed rules, judging from the experience acquired in the years lapsing since the act came into effect.

These regulations are approved, therefore, in acknowledgement of the need to introduce greater consistency in the regulatory legislation with respect to the transposition of the Directive and elaborate further on the innovative aspects of Constitutional Act 15/1999, as well as others where experience has identified the need for greater precision to enhance the legal certainty of the system as a whole.

III

The regulations cover the domain previously protected under Royal Decrees 1332/1994 of 20 June and 994/1999 of 11 June, account taken of the need to establish criteria applicable to non-automatically processed personal data and files. Moreover, the attribution of duties to the Spanish Data Protection Agency in Act 34/2002 of 11 July on Information Society and Electronic Commerce Services and General Act 32/2003 of 3 November on Telecommunications calls for the establishment of procedures under which the Agency may exercise its power to impose penalties.

The regulations are structured around nine titles whose content addresses the essential matters in this area.

Title I deals with the object and scope of application of the regulations. Since Constitutional Act 15/1999 came into effect, the advisability of elaborating on its Article 2, paragraph 2 has become increasingly obvious, in light of the need to clarify what is meant by files and processing related to personal or domestic activities. This point is of particular relevance, inasmuch as such files and processing are excluded from the legislation on personal data protection.

Furthermore, the present regulations contain no provisions on the personal data processing referred to in Article 2, paragraph 3 of the Constitutional Act, which are governed by specific stipulations and special terms laid down, as appropriate, in Constitutional Act 15/1999 itself. Consequently, the legal provisions applicable to these files and processing are retained.

This title also furnishes a series of definitions that contribute to a clear understanding of the regulations themselves, which is particularly necessary in such a technically complex domain as personal data protection. In another vein, it establishes the criterion to be followed to standardise the calculation of the duration of terms and periods with a view to avoiding distinctions in the treatment of private and public sector files.

Title II refers to data protection principles. Of particular importance is the regulation of the way in which consent is obtained, with attention paid to very specific aspects such as electronic communications services and very specially, the capture of minors' data. It likewise offers what can best be defined as processors' by-laws, which will surely contribute to clarifying all aspects of this role. Finally, the provisions in this domain are supplemented by the provisions of Title VIII on security, establishing a consistent framework for processors' conduct.

Title III addresses an essential issue: individuals' rights in this domain. The rights of access, rectification, erasure and objection to processing, according to Constitutional Court sentence 292/2000, constitute legal capacities stemming from the fundamental right of data protection and "serve the cardinal function of this fundamental right: to guarantee the individual's control over his personal data, which is only possible and effective where compliance with the aforementioned duties are imposed on third parties".

Titles IV to VII clarify important aspects for general business, such as the application of specific criteria to certain types of private sector files where required in light of their significance, namely in connection with financial solvency and creditworthiness and files used for advertising and marketing; the suite of material and formal obligations that should induce controllers to create and register files; the criteria and procedures for international data transfers; and, finally, the regulation of an instrument, the standard code, which is destined to play an increasingly essential role in driving development of the fundamental right of data protection.

Title VIII regulates an area essential to the fundamental right of data protection, namely security, which impacts a number of organisational, management and even investment questions in all organisations that process personal data. The impact of the security obligation has made rigour particularly necessary, for a number of highly significant elements converge in this area. On the one hand, the experience deriving from application of Royal Decree 994/1999 provided insight into the difficulties faced by controllers and identified the strong and weak points of those regulations. On the other, the regulations were in need of adaptation in several respects. In this regard, the present regulations attempt to be especially rigorous in the assignment of security levels, the establishment of the measures to be adopted in each case and the revision thereof whenever necessary. Moreover, it lays down the content of and obligations in connection with the maintenance of the security document with greater precision. An attempt has also been made to accommodate the regulations to the many material and personal arrangements for organising security that are found in practice. Lastly, this title regulates a series of measures intended for structured but not automatic files and processing to provide their controllers with a clear framework for action.

Title IX, finally, which describes the procedures to be followed by the Spanish Data Protection Agency, addresses only those specialities that differentiate its procedures from the general procedural rules laid down in Act 30/1992 of 26 November on the Legal Framework for Public Authorities and General Administrative Procedures, whose application is defined to be subsidiary to application of the present regulations.

By virtue whereof, acting on a proposal put forward by the Ministry of Justice, subsequent to approval by the Ministry of Public Administration, pursuant to the agreement of the Council of State and after deliberation by the Council of Ministers at its 21 December 2007 meeting, I hereby.

D E C R E E:

Sole article. Approval of the Regulations.

That the Regulations Relating to Royal Decree 15/1999 of 13 December on Personal Data Protection are adopted, in accordance with the text set out below.

Transitional provision one. Adaptation of the standard codes registered in the General Data Protection Registry.

The Spanish Data Protection Agency must be notified within one year of the entry into force of the present royal decree of any amendments effected in standard codes registered with the General Data Protection Registry to adapt their content to the provisions of Title VII of these regulations.

Transitional provision two. Terms for implementing security measures.

The security measures provided for in the present royal decree shall be implemented in accordance with the rules set out below.

1st. Automatic files existing on the date of entry into effect of the present royal decree shall be subject to the following.

a) Medium level security measures shall be implemented for the files listed below within one year of such entry into effect:

   1. files whose controllers are Social Security management agencies or bodies common to the entire Social Security system and which are related to the competencies thereof

   2. files whose controllers are Social Security work accident and occupational disease mutual companies

   3. files containing a set of personal data that define citizens' characteristics or personalities and provide grounds for evaluating certain personality or behavioural traits, respecting measures for this level of security not required under Article **4.**4 of the Regulations on Security Measures for Automatic Files Containing Personal Data, approved by Royal Decree 994/1999 of 11 June.

b) Medium level security measures for the files listed below shall be implemented within one year and high level security measures within eighteen months of the entry into effect of the present regulations:

   1. files containing data on acts involving gender violence

   2. files whose controllers are operators providing publicly accessible electronic communications services or exploiting public electronic communications networks, in respect of data on traffic and location.

c) In all other cases, when the present regulations call for implementation of an additional measure not provided for in the Regulations on Security Measures for Automatic Files Containing Personal Data, approved by Royal Decree 994/1999 of 11 June, such measure must be implemented within one year of the entry into effect of the present royal decree.

2nd. Non-automatic files existing on the date of entry into effect of the present royal decree shall be subject to the following.

a) Low level security measures must be implemented within one year of its entry into force.

b) Medium level security measures must be implemented within eighteen months of its entry into force.

c) High level security measures must be implemented within two years of its entry into force.

3rd. Both automatic and non-automatic files created after the date of entry into effect of the present royal decree shall have all the security measures regulated hereunder in place from the time of their creation.

Transitional provision three. Transitional system for requests for the exercise of individuals' rights.

Requests for the exercise of the rights of access, objection, rectification or erasure lodged prior to the entry into effect of the present royal decree shall be governed by the previous legislation and not by the present regulations.

Transitional provision four. Transitional arrangements for proceedings underway.

Proceedings instituted prior to the entry into effect of the present royal decree shall be governed by the previous legislation and not by the present regulations.

Transitional provision five. Transitional arrangements for prior action.

Actions instituted prior to the entry into effect of the present royal decree shall be governed by the previous legislation and not by the present regulations.

The present royal decree shall apply to prior actions instituted after its entry into effect.

Sole repealing provision. Repeal of legislation.

Royal Decree 1332/1994 of 20 June Relating to Certain Provisions in Constitutional Act 5/1992 of 29 October on the Regulation of the Automatic Processing of Personal Data, Royal Decree 994/1999 of 11 June Approving the Regulations on Security Measures for Automatic Files Containing Personal Data and all rules of equal or lower rank that conflict with the provisions of the present royal decree are hereby repealed.

Final provision one. Definition of competence.

Title I, with the exception of Article 4, paragraph c), Titles II, III, VII and VIII, as well as Articles 52, 53.3, 53.4, 54, 55.1, 55.3, 56, 57, 58 and 63.3 of these Regulations are decreed under the provisions of Article 149.1st.1 of the Constitution, which attributes to the Central Government exclusive competence to regulate the basic conditions guaranteeing the equality of all Spaniards in the exercise of their rights and compliance with their constitutional duties.

Final provision two. Entry into force.

The present royal decree shall enter into effect three months after its publication in full in the *Official State Journal*.

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

TITLE I

General provisions

Article 1. Object.

1. The present regulations elaborate on Constitutional Act 15/1999 of 13 December on Personal Data Protection.

2. Chapter II of Title IX hereunder also elaborates on the provisions relating to the exercise by the Spanish Data Protection Agency of its power to impose penalties pursuant to the stipulations laid down in Constitutional Act 15/1999 of 13 December, Title VII of Act 34/2002 of 11 July on Information Society and Electronic Commerce Services and Title VIII of General Act 32/2003 of 3 November on Telecommunications.

Article 2. Objective scope.

1. The present regulations shall be applicable to personal data recorded on physical media susceptible to processing and subsequent use of whatsoever nature of these data by the public or private sector.

2. They shall not be applicable to data on bodies corporate or to files including the data on the natural persons engaged thereby that consist in no more than first and last names, duties or positions, postal or electronic address, and professional telephone and fax numbers.

3. Data on individual businesspeople that refer to their engagement in trade, industry or shipping shall likewise be understood to be excluded from the protection afforded personal data.

4. These regulations shall not be applicable to data referring to the deceased. That notwithstanding, individuals related to the deceased by kinship or similar may notify the controllers of files or processing systems containing such data of the death, furnishing due substantiation thereof, and request erasure of the data where in order.

Article 3. Geographic scope.

1. The processing of personal data shall be governed by the present regulations in the following circumstances.

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

   When the preceding conditions are not met but at least one processor is located in Spain, such processor shall be subject to the rules laid down in Title VIII of these regulations.

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.

   In this case the controller shall designate a representative established on Spanish soil.

2. For the intents and purposes of the preceding paragraphs, establishment, irrespective of the legal status thereof, shall be understood to be any stable facility in which real and effective business can be conducted.

Article 4. Data files or processing excluded.

The personal data protection provisions laid down in the present regulations shall not be applicable to the data files and processing listed below.

a) Files kept by natural persons in connection with solely personal or domestic activities.

   Data processing shall only be regarded to be related to personal or domestic activities when it is associated with activities conducted in the framework of individuals' private or family life.

b) Files subject to legislation on the protection of classified information.

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

Article 5. Definitions.

1. For the purposes of these regulations, the terms listed below shall be defined as specified.

a) Data subject shall mean the natural person whose data are processed.

b) Erasure shall mean the procedure whereby the controller ceases to use the data. Data erased shall be blocked, which shall entail the identification and separation thereof to prevent their processing except for use by the public authorities, judges and courts to attend to possible liabilities stemming from their processing, and only for as long as such liabilities are claimable. The data shall be deleted when that term lapses.

c) Data surrender or disclosure shall mean the act of revealing data to anyone other than the data subject.

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

e) Decoupled data item shall mean any item from which a data subject's identity cannot be deduced.

f) Personal data shall mean any numerical, alphabetical, graphic, photographic, acoustic or any other type of information relating to identified or identifiable natural persons.

g) Health-related personal data shall mean information concerning an individual's, past, present or future physical or mental health. In particular, an individual's percentage of disability or genetic information shall be regarded to constitute health-related data.

h) Recipient shall mean the natural or public or private legal person or government body to whom the data are disclosed.

   Organisations with no legal personality who act as differentiated subjects may also be recipients.

i) Processor shall mean the natural or public or private legal person or government body who, solely or jointly with others, processes personal data on behalf of the controller pursuant to a legal relationship between the two that delimits the scope of the service provided by the processor.

   Organisations with no legal personality who act as differentiated subjects may also be processors.

j) Personal data exporter shall mean the natural or public or private legal person or government body located on Spanish soil who transfers personal data to a third country in accordance with the provisions of these regulations.

k) File shall mean any set of structured personal data, irrespective of the manner in which it is generated, stored, organised or accessed, that provides access to the data in accordance with certain criteria.

l) Private sector files shall mean files whose controllers are individuals, private companies or corporations, irrespective of the identity of their shareholders or the origin of their financial resources, and files whose controllers are public corporations when such files are not strictly associated with the exercise of the competencies attributed thereto under specific rules of public law.

m) Public sector files shall mean files whose controllers are constitutional bodies or bodies with constitutional significance either at the national or regional level, regional public authorities and entities or bodies related thereto or under their aegis and public corporations where the purpose of the file is the exercise of competencies under public law.

n) Non-automatic file shall mean any set of personal data not automatically organised or structured in accordance with criteria specifically related to natural persons, that provides access to their data without inordinate effort, be it centralised, decentralised or functionally or geographically distributed.

ñ) Personal data importer shall mean the natural or public or private legal person or government body who, as controller, processor or third party, receives data transferred internationally to a third country.

o) Identifiable person shall mean any person whose identity can be directly or indirectly determined by information referred to his physical, physiological, psychological, economic, cultural or social identity. A natural person shall not be regarded to be identifiable if such identification calls for inordinate amounts of time or effort.

p) Decoupling procedure shall mean any personal data processing procedure that yields decoupled data.

q) Controller shall mean the natural or public or private legal person or government body who alone or jointly with others determines the purpose, content and use of the data, even where not materially involved in their processing.

   Organisations with no legal personality who act as differentiated persons may also be controllers.

r) Third party shall mean a natural or public or private legal person or government body other than the data subject, controller, processor or persons authorised to process data under the controller's or processor's direct authority.

   Organisations with no legal personality who act as differentiated persons may also be third parties.

s) International data transfer shall mean data processing involving the transmission of data outside the European Economic Area, for the purposes of either data surrender or disclosure or of data processing for a controller established on Spanish soil.

t) Data processing shall mean any technical operation or procedure, automatic or otherwise, for data collection, recording, storage, formulation, modification, query, use, modification, erasure, blockage or deletion, as well as the surrender of data deriving from communications, queries, interconnections or transfers.

2. In particular, in connection with the provisions of Title VIII of these regulations, the terms listed below shall be defined as specified.

a) Authorised access shall mean authorisation granted to a user to make use of the resources in question. As appropriate, it shall include authorisations or functions attributed to a user by the controller or security manager.

b) Authentication shall mean the procedure to verify user identity.

c) Password shall mean confidential information, often comprising a string of characters, that may be used for user authentication or to access a resource.

d) Access control shall mean the mechanism whereby data or resources may be accessed depending on the identity authenticated.

e) Backup copy shall mean a copy of data or an automatic file on a medium from which they may be retrieved.

f) Document shall mean any written, graphic, acoustic, video or other manner of information that can be processed in an information system as a differentiated unit.

g) Temporary files shall mean working files created by users or processes and needed for occasional processing or as an intermediate step in data processing.

h) Identification shall mean the procedure whereby user identity is recognised.

i) Incident shall mean any anomaly affecting or that might affect data security.

j) User profile shall mean access authorised for a group of users.

k) Resource shall mean any component part of an information system.

l) Security manager shall mean the person or persons formally designated by the controller to coordinate and control all applicable security measures.

m) Information systems shall mean the set of files, processing operations, software, media and, as appropriate, hardware used to process personal data.

n) Processing system shall mean the manner in which an information system is organised or used. Depending on the processing system, information systems may be automatic, non-automatic or semi-automatic.

ñ) Medium shall mean the physical object that stores or contains data or documents or an object liable to being processed in an information system or to being used to record or retrieve data.

o) Document transmission shall mean transferring, reporting, sending, delivering or disclosing the information contained therein.

p) User shall mean the individual or process authorised to access data or resources. Processes that provide access to data or resources without identifying a natural person as the user shall be regarded to be users.

Article 6. Rules for calculating terms and periods.

Where these regulations specify a term or period in days, only business days shall be computed. When the term or period is given in months, it shall be computed from the day of the first month to same day of the last month.

Article 7. Publicly accessible sources.

1. For the intents and purposes of Article 3, paragraph j) of Constitutional Act 15/1999, only the following shall be regarded to be publicly accessible sources.

a) Open census records, regulated as provided in Constitutional Act 15/1999 of 13 December.

b) Electronic communications service guides, under the terms provided in their specific legislation.

c) Lists of individuals belonging to professional groups containing only names, titles, professions, business activities, academic degrees, professional addresses and group membership status. The professional address may include the full postal address, telephone number, fax number and electronic address. In the case of chartered institutions, membership data may include the associate number, date of affiliation and status of professional practice.

d) Daily newspapers and official journals.

e) The media.

2. For the items listed in the preceding paragraph to be regarded to be publicly accessible sources, consultation thereof must be open to any individual, unhindered by limiting legislation and contingent upon no other requirement than payment of a fee, as appropriate.

TITLE II

Data protection principles

CHAPTER I

Data quality

Article 8. Principles relating to data quality.

1. Personal data must be processed in good faith and legitimately. The use of fraudulent, misleading or illicit means to collect data is prohibited.

2. Personal data may only be collected to fulfil the controller's specific, explicit and legitimate purposes.

3. Personal data processed may not be put to uses incompatible with the purposes for which they were collected.

4. Personal data may only be 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.

5. Personal data must be accurate and kept current to ensure that they correctly reflect the data subject's status at all times. Data provided directly by the data subject shall be regarded to be accurate.

Where personal data subject to processing are wholly or partially inaccurate or incomplete, they shall be erased *ex officio* and replaced with the respective rectified or complete data within ten days of when the inaccuracy is discovered, except where the legislation applicable to the file provides for a specific procedure or term within which such procedure must be performed.

Where the data were previously disclosed, the controller must notify the data recipient of the rectification or erasure within ten days, providing the recipient's identity is known.

Recipients still processing the data shall proceed to rectify or erase the data referred to in the notice within ten days of receipt thereof.

Data subjects need not be notified of such updating of their personal data, without prejudice to the exercise of their rights as recognised in Constitutional Act 15/1999 of 13 December.

The provisions of the present paragraph are understood to be without prejudice to the capacities accorded data subjects further to Title III of these regulations.

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

That notwithstanding, they may be kept for the period in which liability may be claimable in connection with a legal relationship or obligation, the performance of a contract or the application of pre-contractual measures requested by the data subject.

Once the term referred to in the preceding paragraphs lapses, the data may only be stored if they are decoupled, without prejudice to the mandatory blocking provided for in Constitutional Act 15/1999 of 13 December and these regulations.

7. Personal data shall be processed in a manner compatible with the exercise of the rights of access, until such time as erasure is in order.

Article 9. Processing for statistical, historic or scientific purposes.

1. For the purposes of paragraph 3 of the preceding article, personal data processing in pursuit of historic, statistical or scientific objectives shall not be regarded to be incompatible.

Determination of the existence of the objectives referred to in the preceding paragraph shall be subject to the specific legislation for each case, in particular the provisions of Act 12/1989 of 9 May on the Regulation of Public Statistics, Act 16/1985 of 25 June on Spanish Historic Heritage and Act 13/1986 of 14 April on the Furtherance and General Coordination of Scientific and Technical Research, and all provisions related thereto, as well as regional legislation on these matters.

2. By way of exception to the provisions of paragraph 6 of the preceding article, the Spanish Data Protection Agency or, as appropriate, the supervisory authorities of the autonomous communities may, where requested by the controller, pursuant to the procedure established in Title IX, Chapter VII, Section Two of these regulations, agree to the maintenance of certain data in full, in light of their historic, statistical or scientific value, as defined in the legislation listed in the preceding paragraph.

Article 10. Cases in which data processing or surrender is legitimate.

1. Personal data may only be processed or surrendered if the data subject consents thereto in advance.

2. That notwithstanding, personal data may be processed or surrendered with no need for the data subject's consent in the following circumstances.

a) Processing or surrender is authorised by a provision with the status of law or laid down in Community law and in particular where the following conditions are met:

   where the purpose of processing or surrender is the pursuit of the controller's or recipient's legitimate interest under cover of such legislation, except where data subjects' interest or fundamental rights and freedoms laid down in Constitutional Act 15/1999 of 13 December prevail

   the data must be processed or surrendered for the controller to comply with an obligation imposed by one of such provisions.

b) (Repealed)[1].

3. Personal data may be processed with no need to obtain the data subject's consent in the circumstances set out below.

a) When they are collected to fulfil public authorities' duties within the scope of the competencies attributed thereto by a provision with the status of law or laid down in Community law.

b) When they are requested by the controller in connection with the conclusion of an agreement or pre-agreement with the data subject or the existence of a business, employment or administrative relationship to which the data subject is a party, and are required to maintain the relationship or implement the agreement.

c) When the purpose of processing the data is to protect the data subject's vital interests under the terms of Article 7, paragraph 6 of Constitutional Act 15/1999 of 13 December.

4. Personal data may be surrendered with no need to obtain the data subject's consent in the following circumstances.

a) Surrender forms part of a freely accepted legitimate legal relationship whose implementation, compliance and enforcement call for data disclosure. In this case disclosure shall only be legitimate when limited to the purpose that warrants such action.

[1] Paragraph 2.b) repealed pursuant to SC Sentences of 8 February 2012

b) The data that must be disclosed are intended for the Ombudsman, the Public Prosecutor, judges, courts, the Court of the Exchequer in the exercise of the duties attributed thereto, or regional institutions with attributions analogous to the duties of the Ombudsman or the Court of the Exchequer.

c) Surrender between public authorities when any of the following conditions are met.

The data are processed for historic, statistical or scientific purposes.

The personal data were collected or compiled by one public authority for another.

The data are disclosed for the exercise of identical competencies or that are related to the same matters.

5. Specially protected data may be processed and surrendered under the terms laid down in Articles 7 and 8 of Constitutional Act 15/1999 of 13 December.

In particular, the data subject's consent shall not be required for the disclosure of personal data on health among National Health System bodies, centres and services, even using electronic media, when the objective is health care for individuals, pursuant to the provisions of Chapter V of Act 16/2003 of 28 May on National Health System Cohesion and Quality.

Article 11. Verification of data in applications submitted to public authorities.

(Cancelled)

CHAPTER II

Consent to data processing and duty to inform

SECTION 1. OBTAINING THE DATA SUBJECT'S CONSENT

Article 12. General principles.

1. The controller shall obtain the data subject's consent to process his personal data except where the legislation stipulates otherwise.

The request for consent must be referred to a specific processing operation or series of processing operations, delimiting the purpose for which consent is requested and all other conditions involved in such operation or series of operations.

2. When the data subject is asked to consent to the surrender of his data, he must be unequivocally informed of the intended use of the data to whose disclosure he is asked to consent and the type of business conducted by the recipient. Consent shall otherwise be null and void.

3. Proof of the existence of the data subject's consent, based on any manner of admissible evidence, shall be incumbent upon the controller.

Article 13. Consent for processing data on minors.

1. Data on individuals over the age of fourteen may be processed with their consent, except where the law requires that such consent may only be given where the minor is assisted by the holders of *patria potestas* or tutelage. Where individuals under the age of fourteen are involved, parental or tutorial consent shall be required.

2. Minors may under no circumstances be asked to provide information on other family members or family

characteristics, such as their parents' occupation, financial information, sociological or any other manner of data, without the consent of the individuals concerned. Data on the father's, mother's or tutor's identity and address may be requested, however, for the sole purpose of obtaining the authorisation stipulated in the preceding paragraph.

3. Information provided to minors whose data are processed must be expressed in a language readily comprehensible thereto and explicitly mention the points stipulated in this article.

4. The implementation of procedures to verify the minor's age and the authenticity of parents', tutors' or legal representatives' consent shall be incumbent upon the controller.

Article 14. Procedure for requesting consent.

1. The controller may request data subjects' consent in the manner established in this article, except where explicit consent for processing data is required by law.

2. The controller may approach data subjects and notify them of the information specified in Article 5 of Constitutional Act 15/1999 of 13 December and Article **12.**2 of these regulations. Subjects shall be granted thirty days in which to express their refusal to have their data processed and advised that unless they notify the controller otherwise, they will be understood to consent to the processing of their personal data.

In particular, where controllers provide data subjects a service that generates periodic or reiterated information or periodic billing, such notification may be included in the aforementioned periodic correspondence, provided it is clearly visible.

3. The controller must be able to ascertain whether notification has been returned for whatsoever reason, in which case the subject's data may not be processed.

4. Data subjects must be provided a simple and cost-free refusal procedure. In particular, procedures shall be regarded to conform to the present regulations when refusal may be expressed, among others, by pre-paid post addressed to the controller or a cost-free telephone call to the respective customer service.

5. When data subjects' consent is requested under the procedure established in this article, it may not be requested again with respect to the same processing operations and for the same purposes until one year has lapsed from the date of such request.

Article 15. Request for consent in the framework of a contractual relationship for purposes not directly related thereto.

If the controller requests the data subject's consent during negotiations to conclude an agreement for purposes not directly related to the maintenance, performance or enforcement of the contractual relationship, the subject must be afforded the opportunity to explicitly refuse to have his data processed or disclosed.

In particular, such obligation shall be understood to be fulfilled when the data subject is allowed to fill in a clearly visible space, which is not previously marked on the document provided to formalise the agreement, or some equivalent procedure is established whereby he can express his refusal to the processing of his data.

Article 16. Data processing for the use and billing of electronic communications services.

Requests for consent to processing or surrendering data on use, billing and location where required, or as appropriate, revocation of such consent pursuant to the legislation governing telecommunications, shall be subject to the specific provisions in that regard and any provisions of this section that do not conflict therewith.

Article 17. Revocation of consent.

1. Data subjects shall be able to revoke their consent by a simple, cost-free method in which the controller earns no revenue whatsoever. In particular, procedures shall be regarded to conform to the present regulations when

such refusal may be notified, among others, by pre-paid post addressed to the controller or a cost-free telephone call to the respective customer service.

Procedures established by the controller for notification by subjects of their refusal to have their data processed consisting of registered letter or similar, telecommunications services that entail surcharges or any other method involving additional costs for data subjects shall not be regarded to conform to the provisions of Constitutional Act 15/1999 of 13 December.

2. The controller shall cease to process data within no more than ten days counting from the receipt of revocation of consent, without prejudice to the obligation to block the data further to the provisions of Article **16.**3 of Constitutional Act 15/1999 of 13 December.

3. When data subjects ask the controller to confirm that their data are no longer being processed, the former must provide an explicit reply.

4. Where the data concerned were surrendered prior to revocation of consent, the controller shall notify the recipients of the revocation within the term specified in paragraph 2. Recipients still processing the data must cease to do so, further to Article 16**.**3 of Constitutional Act 15/1999 of 13 December.

SECTION 2. DUTY TO INFORM DATA SUBJECTS

Article 18. Substantiation of compliance with the duty to inform.

(Cancelled).

Article 19. Special circumstances.

Data may not be surrendered on the occasion of a change in the controller's identity as a result of a merger, spin-off, global surrender of assets and liabilities, uptake or transfer of business activity or a division thereof, or any other corporate restructuring of a similar nature provided for in mercantile legislation. The foregoing is understood to be without prejudice to compliance by the controller with the provisions of Article 5 of Constitutional Act 15/1999 of 13 December.

CHAPTER III

Processor

Article 20. Controller-processor relations.

1. Where data must be accessed by a processor to provide the controller processing services, such access shall not be regarded to constitute data disclosure, providing the provisions of Constitutional Act 15/1999 of 13 December and of the present chapter are met.

The service provided by the processor may be remunerated or otherwise, temporary or permanent.

Data disclosure shall be regarded to exist, however, when the purpose for accessing such data is the establishment of a new relationship between the processor accessing the data and the data subject.

2. When hiring a service that entails personal data processing subject to the provisions of the present chapter, the controller must ensure that the processor is able to guarantee compliance with the provisions of these regulations.

3. If the processor uses the data for some other purpose, discloses them or uses them in breach of the stipulations of the agreement referred to in Article 12, paragraph 2 of Constitutional Act 15/1999 of 13 December, he shall also be regarded to be the controller and be held accountable for any infringements personally committed.

The processor shall incur no liability when, further to the controller's explicit instructions, he discloses the data to a third party identified by the controller and commissioned thereby to provide a service in accordance with the provisions of the present chapter.

Article 21. Service subcontracting.

1. The processor may not subcontract any processing services commissioned by the controller except where he obtains authorisation from the latter to do so. In such event, the service must be hired on behalf and in the stead of the controller.

2. Notwithstanding the provisions of the preceding paragraph, services may be subcontracted subject to compliance with the following requirements.

a) The contract must specify which services may be subcontracted and, where possible, the identity of the company subcontracted.

   When the subcontractor is not identified in the contract, the processor shall be bound to notify the controller of the identity details prior to proceeding to subcontract the services.

b) The subcontractor processes the personal data in conformity with the controller's instructions.

c) The processor and the subcontractor conclude a formal agreement in the terms laid down in the preceding article.

   In that case, the subcontractor shall be regarded to be the processor and shall be subject to the provisions of Article 20.3 of these regulations.

3. If, while the service is being provided, some part thereof should need to be subcontracted and that circumstance is not envisaged in the contract, the provisions of the preceding paragraph shall be applied to the controller.

Article 22. Data storage by the processor.

1. Upon conclusion of the service defined in the agreement, the personal data must be destroyed or returned to the controller or the processor designated thereby, together with any media or documents containing any personal data processed.

Data shall not be destroyed where storage is legally required, in which case they must be returned to the controller, who shall be responsible for their storage.

2. The processor shall duly block and keep data relating to liabilities that may derive from his relationship with the controller.

TITLE III

Rights of access, rectification, erasure and objection

CHAPTER I

General provisions

Article 23. Very personal status.

1. The rights of access, rectification, erasure and objection are absolutely personal and must be exercised by the data subject.

2. Such rights shall be exercised as specified below.

a) By the data subject, who must substantiate his identity as provided in the following article.

b) When the data subject is a minor or otherwise incapacitated to exercise such rights personally, they may be exercised by his legal representative, who must substantiate his capacity as such.

c) These rights may also be exercised through a voluntary representative explicitly designated for that purpose. In such case, the principal's identity must be clearly substantiated in the form of a copy of his national identity card or equivalent document, along with the proxy issued thereby.

When the controller is a public authority or a judiciary body, the proxy may be substantiated by any lawfully valid and reliably verifiable method or a personal statement made in situ by the data subject.

3. Such rights shall be denied when formulated by anyone other than the data subject unable to substantiate that he acts in representation thereof.

Article 24. General conditions for exercising the rights of access, rectification, erasure and objection.

1. Inasmuch as the rights of access, rectification, erasure and objection are independent rights, the exercise of any one may not be understood to be subject to the exercise of any other.

2. Data subjects must be afforded a simple and cost-free procedure to exercise their rights of access, rectification, erasure and objection.

3. Data subjects must be able to exercise their rights of access, rectification, erasure and objection cost-free and under no circumstances may the exercise of such rights entail additional revenues for the controller concerned.

Establishment by the controller of procedures for data subjects' exercise of their rights that consist of registered letters or similar or telecommunications services involving a surcharge or any other means signifying excessive cost for data subjects shall not be regarded to conform to the provisions of Constitutional Act 15/1999 of 13 December or the present regulations.

4. When the controller offers support services for his clientele or for lodging complaints relating to his products or services, he may make those services available to data subjects desiring to exercise their rights of access, rectification, erasure or objection. In such cases, the data subject's identity shall be regarded to be substantiated when he complies with the requisites established by the controller to identify customers for the purposes of service provision or product sales.

5. The controller shall respond to data subjects' requests for access, rectification, erasure or objection even when the latter fail to use the procedure specifically established by the controller, providing they use a means by which dispatch and receipt of the request can be substantiated and the request contains the elements listed in the following article.

Article 25. Procedure.

1. Except in the circumstance referred to in paragraph 4 of the preceding article, rights must be exercised via correspondence addressed to the controller, which must contain the following.

a) The data subject's first and last names; photocopy of his and, as appropriate, his representative's national identity card or passport or other valid identity document or equivalent electronic documents; and the document or electronic instrument substantiating such representation. The use of the data subject's digital signature shall exempt him from furnishing photocopies of his national identity card or equivalent document.

   The preceding paragraph shall be understood without prejudice to the specific legislation applicable to identity data verification by public authorities in administrative procedures.

b) Specific request.

c) Address for notification, date and data signature of the party concerned.

d) Documents substantiating the request, if any.

2. The controller must reply to all requests received, regardless of whether or not the data subject's personal data are included in his files.

3. Where the request does not comply with all the requirements listed in paragraph one above, the controller shall request rectification.

4. The controller's reply must meet the requirements for each case laid down in the present title.

5. The burden of proof of compliance with the duty to reply referred to in paragraph 2 shall be incumbent upon the controller, who must keep substantiation of such compliance.

6. The controller must adopt the necessary measures to guarantee that the individuals in his organisation with access to personal data are able to inform data subjects of the procedures to follow to exercise their rights.

7. The exercise of the rights of access, rectification, erasure and objection may be modulated for reasons of public safety under the circumstances and within the scope defined by law.

8. When laws applicable to certain specific files establish a special procedure for the rectification or erasure of the data contained therein, those provisions shall prevail.

Article 26. Requests addressed to a processor.

When data subjects address a processor to exercise or request the exercise of their rights, the processor must refer the request to the controller for action, unless the arrangement governing the relationship between the two provides that the processor shall attend to data subjects' requests to exercise their rights of access, rectification, erasure or objection on the controller's behalf.

CHAPTER II

Right of access

Article 27. Right of access.

1. The right of access is the data subject's right to ascertain whether his personal data are being processed and the purpose for which they are processed, as appropriate, and to obtain any information available on the origin of such data and the past or planned disclosure thereof.

2. By virtue of the right of access, the data subject may obtain information from the controller on specific data, the data included in a given file, or the entire set of data referring to him and processed by the controller.

When warranted by reasons of particular complexity, however, the controller may ask the data subject to specify the files with respect to which he wishes to exercise his right of access. The latter shall provide a list of such files to such end.

3. The right of access is independent of the right granted to data subjects under special laws and in particular Act 30/1992 of 26 November on the Legal Framework for Public Authorities and General Administrative Procedures.

Article 28. Exercise of the right of access.

1. When exercising their right of access, data subjects may opt to receive the information by consulting the file in one or several manners:

a) Visualisation on a screen

b) Written communication, copy or photocopy sent by post, registered or otherwise

c) Fax

d) Electronic mail or other forms of electronic correspondence

e) Any other system offered by the controller and suited to the file setup or the nature or material implementation of the processing operations.

2. The file consultation systems referred to in the preceding paragraph may be restricted in keeping with the file setup or nature or material implementation of the processing operations, providing the systems available to data subjects are cost-free and written information can be obtained therefrom wherever requested.

3. When providing access, the controller must comply with the provisions of Title VIII of these regulations.

If the data subject rejects a system for exercising the right of access offered by the controller, the latter shall not be liable for the possible security risks to the information that may stem from the data subject's chosen alternative.

Similarly, if the controller provides a procedure for exercising the right of access and the data subject demands the implementation of a procedure that entails inordinate costs but yields the same results and guarantees the same level of security as the procedure proposed by the controller, the costs deriving from that choice shall be defrayed by the data subject.

Article 29. Allowance of access.

1. The controller shall rule on requests for access within no more than one month counting from the date of receipt thereof. When that term lapses and no explicit reply to the request for access is forthcoming, the data subject may lodge the claim described in Article 18 of Constitutional Act 15/1999 of 13 December.

If the controller has no personal data on the data subjects concerned, he must notify them to that effect within the term referred to above.

2. If the request is granted and the controller fails to include the information referred to in Article 27.1 in his correspondence, effective access shall be granted within ten days of such correspondence.

3. The information furnished, regardless of the medium used, shall be legible and intelligible and free of codes that call for the use of specific hardware.

The aforementioned information shall include the subject's raw data, any data resulting from computer handling or processing, as well as all available information on the origin of the data, the recipients thereof and a description of the specific uses and purposes for which the data are stored.

Article 30. Denial of access.

1. The controller may deny access to personal data when that right was exercised in the twelve months prior to the request, except where a legitimate interest in this regard is substantiated.

2. Access may also be denied where provided by domestic law or directly applicable Community law or when either prevents the controller from revealing the data involved to the data subjects.

3. The controller shall inform data subjects, without exception, of their right to request legal protection from the Spanish Data Protection Agency or, as appropriate, from the regional supervisory authorities further to the provisions of Article 18 of Constitutional Act 15/1999 of 13 December.

CHAPTER III

Rights of rectification and erasure

Article 31. Rights of rectification and erasure.

1. The right of rectification is data subjects' right to the modification of inaccurate or incomplete data.

2. The exercise of the right of erasure shall entail the deletion of inappropriate or excessive data, without prejudice to the duty to block data laid down in these regulations.

Where data subjects exercise their right of erasure to revoke consent previously granted, the provisions of Constitutional Act 15/1999 of 13 December and these regulations shall apply.

Article 32. Exercise of the rights of rectification and erasure.

1. The request for rectification must specify the data concerned and the correction to be made and must include documents justifying the request.

In requests for erasure, data subjects must specify the data concerned and furnish the documents justifying the request, as appropriate.

2. The controller shall rule on the request for rectification or erasure within no more than ten days counting from the date of receipt thereof. When that term lapses and no explicit reply to the request is forthcoming, the data subject may lodge the claim described in Article 18 of Constitutional Act 15/1999 of 13 December.

If the controller has no personal data on the data subjects concerned, he must notify them to that effect within the term referred to above.

3. If the data rectified or erased had been previously surrendered, the controller must notify the recipient of the rectification or erasure within the aforementioned term, and the latter must likewise proceed to rectify or erase the data within ten days counting from the date of receipt of the controller's notification.

Data subjects need not be notified of rectification or erasure of their personal data by the recipient, without prejudice to the exercise of their rights as recognised in Constitutional Act 15/1999 of 13 December.

Article 33. Denial of the rights of rectification and erasure.

1. Erasure shall not be in order when personal data must be kept for the period of time provided in the applicable legislation or, as appropriate, in the agreements between the controller and the data subject that gave rise to the data processing operation.

2. The rights of rectification and erasure may also be denied where provided by a domestic or directly applicable Community law or when either prevents the controller from revealing the data involved to the data subjects.

3. The controller shall inform data subjects, without exception, of their right to request legal protection from the Spanish Data Protection Agency or, as appropriate, from the regional supervisory authorities further to the provisions of Article 18 of Constitutional Act 15/1999 of 13 December.

CHAPTER IV

Right of objection

Article 34. Right of objection.

The right of objection is data subjects' right to prevent or halt the processing of their personal data in the circumstances set out below.

a) When their consent to the processing operation is not required, as a result of compelling and legitimate grounds relating to their personal situation that warrant such action, except where otherwise provided by law.

b) When files whose purpose is advertising and marketing, as provided in Article 51 of these regulations, regardless of the identity of the company responsible for their creation.

c) When the purpose of processing the data is the adoption of a decision affecting the data subjects, based solely on the automatic processing of their personal data, as provided in Article 36 of these regulations.

Article 35. Exercise of the right of objection.

1. The right of objection shall be exercised by a request addressed to the controller.

When the objection is based on sub-paragraph a) of the preceding paragraph, the request must contain an account of the compelling and legitimate grounds relating to the data subject's personal situation that warrant exercise of this right.

2. The controller shall rule on the request for objection within no more than ten days counting from the date of receipt thereof. When that term lapses and no explicit reply to the request is forthcoming, the data subject may lodge the claim described in Article 18 of Constitutional Act 15/1999 of 13 December.

If the controller has no personal data on the subjects concerned, he must notify them to that effect within the term referred to above.

3. The controller must either exclude the data on the subjects exercising their right of objection from the processing operation or explain the reasons for denying their request within the term stipulated in paragraph 2 of this article.

Article 36. Right to object to decisions based solely on automatic data processing.

1. Data subjects are entitled to refuse to be bound by decisions that carry legal or otherwise significant effects, based solely on data processing designed to evaluate certain personality or behavioural traits, such as job performance, credit rating, reliability or conduct.

2. That notwithstanding, data subjects may be bound by the decisions described in paragraph 1 under the following circumstances.

a) When the decision was adopted in the framework of an agreement concluded or performed at the data subject's request, providing he is allowed the opportunity to put forward any allegations he deems relevant for

the defence of his rights or interests. The controller must always inform the data subject in advance, clearly and precisely, that decisions will be made as described in paragraph 1 and shall erase the data if the agreement is not ultimately concluded.

b) When the decision is authorised by a provision with the status of law establishing measures that guarantee the data subject's legitimate interest.

TITLE IV

Provisions applicable to certain private sector files

CHAPTER I

Files containing information on financial solvency and creditworthiness

SECTION 1. GENERAL PROVISIONS

Article 37. Applicable legislation.

1. The processing of personal data on financial solvency and creditworthiness provided for in Article 29, paragraph 1 of Constitutional Act 15/1999 of 13 December, shall be generally subject to the provisions of that constitutional act and the present regulations.

2. For the files referred to in the preceding paragraph, exercise of the rights of access, rectification, erasure and objection shall be governed by the provisions of Title III, Chapters I to IV of these regulations, further to the following criteria.

a) When requests to exercise such rights are addressed to the controller, he shall be bound to honour them regardless of the circumstances.

b) When requests are addressed to persons and entities who use the service, they must inform the data subject of the data relating thereto that have been disclosed to them and furnish the identity of the controller to enable the data subject to apply to the controller to exercise his rights.

3. Further to Article 29, paragraph 2 of Constitutional Act 15/1999 of 13 December, 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 may also be processed.

These data must be kept in files created for the exclusive purpose of providing credit information on the data subject and processing thereof shall be governed by these regulations and in particular the provisions of the Section Two of the present chapter.

SECTION 2. PROCESSING OF 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

Article 38. Requisites for inclusion of data.

1. Only personal data that are determinant for judging the data subject's financial solvency may be included in these files, and only providing the following requirements are met.

a) Prior default on an indisputable, mature and callable debt, *with respect to which no legal, arbitrational or administrative proceedings have been instituted or, where financial services are concerned, no claim has been lodged in the terms established in the Regulations on Financial Service Customers' Ombudsmen enacted under Royal Decree 303/2004 of 20 February.*

b) Lapse of less than six years from the date on which the debt should have been paid or since the obligation or specific instalment, in the event of periodic maturity, fell due.

c) Service of a prior claim for payment upon the debtor.

2. (Cancelled)

3. The creditor or the party acting on his behalf or in his interest shall be bound to keep sufficient evidence of compliance with the requisites established in this article and of the claim for payment referred to in the following article, which shall be available to the controller of the collective file and the Spanish Data Protection Agency.

Article 39. Information prior to inclusion.

The creditor must inform the debtor upon conclusion of the agreement and without exception when issuing the claim referred to in paragraph 1, sub-paragraph c) of the preceding article, that if payment is not made on the due date and if the requisites set out in such article are met, the data on the delinquent payment may be entered into files on compliance or non-compliance with financial obligations.

Article 40. Notification of inclusion.

1. Data subjects whose personal data have been recorded in such a collective file must be notified thereof by the controller within thirty days of data entry, and likewise informed of their entitlement to exercise the rights of access, rectification, erasure and objection in the terms laid down in Constitutional Act 15/1999 of 13 December.

2. A notice shall be served for each specific debt, regardless of whether it involves the same or different creditors.

3. The notice must be served by a reliable and traceable means independent of the notifying entity, enabling the latter to substantiate delivery thereof.

4. The controller must be able to ascertain, at all times, whether the notice has been returned for whatsoever reason, in which case the subject's data may not be processed.

Notices returned as a result of the addressee's refusal to receive them shall not be understood to constitute sufficient grounds for refraining from processing the respective subject's data.

5. If the notice on inclusion in the collective file is returned, the controller thereof shall apply to the creditor to verify the concurrence of the address used to serve such notice and the address covenanted in the agreement with the client for the purposes of correspondence and shall refrain from processing the data if the creditor fails to confirm the accuracy of that information.

Article 41. Data validity period.

1. Only data accurately reflecting the status of debts at any given time may be processed.

All data relating to a debt shall be erased immediately upon payment or settlement thereof.

2. In all other cases, the data must be erased six years after maturity of the obligation or of the specific instalment in the event of periodic due dates.

Article 42. Access to information in the file.

1. Data in the collective file may only be consulted by third parties when they need to ascertain the data subject's financial solvency. In particular, such circumstance shall be understood to exist in the following cases.

a) The data subject maintains some manner of contractual relationship with the third party that has not yet matured.

b) The data subject intends to conclude an agreement with the third party that entails deferred payment of the price.

c) The data subject intends to conclude an agreement with the third party for the provision of a periodically billed service.

2. Data subjects to whom the conditions described in sub-paragraphs b) and c) above are applicable must be informed, in writing, of the third parties' right to consult the file by the parties so entitled.

Where the products or services referred to in the preceding paragraph are acquired by telephone, such information need not be furnished in writing. The burden of proof of compliance with the duty to inform shall be incumbent upon the third party.

Article 43. Liability.

1. The creditor or the party acting on his behalf or in his interest must ensure that all the requisites laid down in Articles 38 and 39 are met when notifying the controller of the collective file of adverse data.

2. The creditor or the party acting on his behalf or in his interest shall be held liable for furnishing groundless or inaccurate data for inclusion in the file, under the terms set out in Constitutional Act 15/1999 of 13 December.

Article 44. Exercise of the rights of access, rectification, erasure and objection.

1. The exercise of the rights of access, rectification, erasure and objection shall be governed by the provisions of Title III, Chapters I to IV o these regulations, without prejudice to the stipulations of the present article.

2. The exercise by data subjects of their right of access to data included in a file regulated by Article 29.2 of Constitutional Act 15/1999 of 13 December shall be governed by the rules listed below.

1st. When requests are addressed to the controller of the collective file, he must furnish data subjects with all the data thereon present in the file.

In that case, in addition to complying with the stipulations of the present regulations, the controller of the collective file must furnish data subjects with the assessments and appraisals referring thereto in the last six months and the name and address of the recipients.

2nd. If requests are addressed to an institution participating in the system, the institution in question must furnish data subjects with all the data thereon to which they have access, as well as the identity and address of the controller of the collective file for the purposes of full exercise of their right of access.

3. When data subjects exercise their right of rectification or erasure of data included in a file regulated by Article 29.2 of Constitutional Act 15/1999 of 13 December, the rules listed below shall be followed.

1st. If the requests are addressed thereto, the controller of the collective file shall take the necessary measures to transfer such requests to the institution that furnished the data, which shall proceed accordingly. If no reply is received from the institution within seven days, the controller of the collective file shall proceed to cautionary rectification or erasure of the data in question.

2nd. If the requests are addressed to the party who furnished the data in the collective file, such party shall proceed to rectify or erase the data in his files and to notify the controller of the collective file thereof in ten days and reply as well to the data subject in the terms set out in Article 33 of these regulations.

3rd. If the request is addressed to an institution participating in the system that did not furnish the data in the collective file, such institution shall inform the data subject accordingly within no more than ten days, and provide him with the identity and address of the controller of the collective file for the purposes of submitting his request to exercise his rights to such controller.

CHAPTER II

Processing for advertising and marketing

Article 45. Data liable to be processed and information for the data subject.

1. Persons engaging in compiling addresses, distributing documents, advertising, distance selling, marketing or similar activities and those who engage in such activities to market their own or third parties' products or services, may use names and addresses and other personal data only where one of the following circumstances applies.

a) The data are listed in one of the publicly accessible sources referred to in Article 3, paragraph j) of Constitutional Act 15/1999 of 13 December and article 7 of these regulations and the data subject has not objected to or refused to allow the processing of his data for the activities described in this paragraph.

b) The data were furnished by the subjects themselves or obtained with their consent for specific, explicit and legitimate advertising or marketing purposes, and the data subjects were informed of the specific industries and businesses about which they might receive information or advertising.

2. When the data are taken from publicly accessible sources and intended for advertising or marketing, all correspondence addressed to the data subject shall include information on the source of the data, the identity of the controller, the rights to which the data subject is entitled and the identity of the party to whom he may apply to exercise such rights.

For these intents and purposes, the data subject must be informed that his data were obtained from publicly accessible sources and the entity from which they were obtained.

Article 46. Data processing in advertising campaigns.

1. Organisations may only advertise their own products or services among their customers where their data processing operations concur with one of the circumstances laid down in Article 6 of Constitutional Act 15/1999 of 13 December.

2. Where an organisation hires or commissions third parties to conduct an advertising campaign for its products or services, and also commissions the processing of certain data, the following rules shall apply.

a) When the parameters identifying the campaign recipients are established by the institution for whom the campaign is conducted, that institution shall be the controller.

b) When the parameters are determined solely by the institution or institutions conducting the campaign, such institutions shall be the controller.

c) When both types of institution contribute to determining the parameters, both shall be controllers.

3. In the circumstance described in the preceding paragraph, the institution commissioning the advertising campaign shall adopt the necessary measures to ensure that when obtaining the data, the contractor institution complies with the requisites laid down in Constitutional Act 15/1999 of 13 December and the present regulations.

4. For the intents and purposes of the present article, recipients' identifying parameters shall be regarded to be the variables used to identify the target audience and delimit the individual members of that audience in a campaign or marketing operation for products or services.

Article 47. Personal data cleansing.

When two or more controllers, on their own initiative or commissioned by third parties, cross-process their files

without the data subjects' consent in an attempt to determine which data subjects are customers of one or the other or several of these institutions for the purposes of advertising or marketing their products or services, such processing shall constitute data surrender or disclosure.

Article 48. Files to be excluded from commercial correspondence.

Controllers notified of data subjects' refusal to receive advertising may keep the minimum data necessary to identify such subjects and adopt the necessary measures to prevent advertising from being sent to them.

Article 49. Collective files for exclusion from commercial correspondence.

1. General or industry-wide collective files may be created for the purpose of processing the personal data necessary to prevent the dispatch of commercial correspondence to data subjects refusing to receive advertising or objecting to the receipt thereof.

To these ends, the files may contain the minimum data needed to identify such subjects.

2. When a data subject notifies a specific controller of his refusal to allow the processing of his data for advertising or marketing purposes or his objection thereto, he must be informed of the existence of collective general or industry-specific files of excluded subjects, as well as the identity and address of the controller and the purpose of the processing operation.

Data subjects may request their exclusion from a specific file or processing operation or their inclusion in general or industry-specific collective files listing excluded subjects.

3. The controller of the collective file may process the data on subjects refusing to allow the processing of their data for advertising or marketing purposes or objecting thereto, providing all the other obligations established in Constitutional Act 15/1999 of 13 December and the present regulations are observed.

4. Parties intending to process data for advertising or marketing purposes must first consult the collective files that may be applicable to such processing, to ensure they do not process the data of subjects objecting to or refusing to allow such processing.

Article 50. Rights of access, rectification and erasure.

1. The exercise of the rights of access, rectification and erasure in connection with processing operations for advertising and marketing purposes shall be subject to the provisions of Title III, Chapters I to IV of these regulations.

2. If the data subject lodges his request to exercise his right with the entity that commissioned an advertising campaign from a third party, the entity in question shall be bound to notify the controller of such request within ten days of receipt thereof, and the controller shall submit to the data subject's right within ten days of the receipt of such notice and inform the data subject accordingly.

The provisions of the preceding paragraph shall be understood to be without prejudice to the requirement laid down in Article 5.5, paragraph two of Constitutional Act 15/1999 of 13 December and incumbent upon the advertiser.

Article 51. Right of objection.

1. Data subjects shall be entitled to object to the processing of their data via cost-free request, in response to which their data shall be erased and removed from the processing operation.

The objection referred to in the preceding paragraph must be understood without prejudice to the data subject's right to revoke any consent granted to process is data at his discretion.

2. To this end, the data subject must be afforded a simple and cost-free means for objecting to the processing of his data. In particular, the provisions of this paragraph shall be regarded to be met when such rights can be exercised by a making a cost-free telephone call or sending e message by electronic mail.

3. When the controller offers support services for his clientele or for lodging complaints relating to his products or services, he may make those services available to data subjects desiring to exercise their right of objection.

Establishment by the controller of procedures for data subjects' exercise of their right of objection that consist of registered letters or similar or telecommunications services involving a surcharge or any other means signifying excessive cost for data subjects shall not be regarded to conform to the provisions of Constitutional Act 15/1999 of 13 December or the present regulations.

The exercise of data subjects' rights may not under any circumstances entail additional revenues for the controller involved.

4. If the data subject lodges his request to exercise his right of objection with the entity that commissioned an advertising campaign from a third party, the entity in question shall be bound to notify the controller of the such request within ten days of receipt thereof, and the controller shall submit to the data subject's right within ten days of the receipt of such notice and inform the data subject accordingly.

The provisions of the preceding paragraph shall be understood to be without prejudice to the requirement laid down in Article 5.5, paragraph two of Constitutional Act 15/1999 of 13 December and incumbent upon the advertiser.

TITLE V

Pre-processing obligations

CHAPTER I

Creation, modification or deletion of public sector files

Article 52. Provision or decision on file creation, modification or deletion.

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

2. The provision or decision must be decreed and published prior to file creation, modification or deletion.

Article 53. Form of the provision or decision.

1. When the provision refers to Central Government bodies or entities or agencies under its aegis, it must adopt the form of a ministerial order or resolution issued by the head of the respective entity or agency.

2. Where State constitutional bodies are concerned, the provisions of the respective regulations shall prevail.

3. The legislation specific to each case shall also prevail when the entities responsible are autonomous communities, local corporations, entities or agencies under their aegis, public universities or regional bodies with duties analogous to the duties of State constitutional bodies.

4. The creation, modification or deletion of the files whose controllers are public law corporations and related to the exercise thereby of public law competencies must be effected by decision of their governing bodies in the terms established in their respective by-laws and must be published in the *Official State Journal* or respective official journal.

Article 54. Content of the provision or decision.

1. Provisions or decisions on file creation must contain the following items.

a) The identification of the file or processing operation, specifying denomination and a description of its purpose and expected use.

b) The origin of the data, specifying the community of individuals to be asked to furnish their personal data or who are obliged to do so, the procedures for collecting the data and the source thereof.

c) The basic structure of the file, consisting of a detailed description of identity data and, as appropriate, of specially protected data, as well as all other categories of personal data included therein and the processing system used to organise the data.

d) Planned data disclosure, if any, specifying the recipients or categories of recipients.

e) Planned international data transfers to third countries, if any, specifying the countries hosting the data.

f) The controllers.

g) The services or units to be addressed to exercise the rights of access, rectification, erasure and objection.

h) The low, medium or high security level required under the provisions of Title VIII of the present regulations.

2. Provisions or agreements modifying files shall specify the modifications to be made to any of the items listed in the preceding paragraph.

3. The provisions or agreements decreed to delete files shall establish the destination thereof or, as appropriate, the measures to be adopted to destroy them.

CHAPTER II

Notification and registration of private or public sector files

Article 55. File notification.

1. All competent authorities controlling public sector files shall notify the Spanish Data Protection Agency of any files containing personal data for the purpose of registration in the General Data Protection Registry within thirty days of publication of the provision or decision creating the file in the respective official journal.

2. Individuals or private entities intending to create private sector personal data files shall notify the Spanish Data Protection Agency thereof prior to proceeding to their creation. Such notification shall specify the identity of the controller and the file, the purpose and planned use, the processing system used in their organisation, the community of people whose data are to be obtained, the procedures for collecting the data and their origin, the data categories, the access service or unit, specification of the low, medium or high level security measures required and, as appropriate, the identity of the processor where the file is located as well as of the recipients of data surrendered or internationally transferred.

3. When the obligation to report the creation of files affects files subject to the supervision of a regional supervisory authority that has created its own file registry, the notification shall be submitted to the competent regional authority, which shall in turn refer the information to the General Data Protection Registry for registration.

The General Data Protection Registry may either call upon the regional supervisory authorities to proceed to the referrals mentioned in the preceding paragraph or include such files in the Registry *ex officio*.

4. The notification procedure shall be as established in Title IX, Chapter IV, Section One of these regulations.

Article 56. Data processing on different media.

1. Notification of personal data files must be submitted regardless of the processing system and medium or media used for their organisation.

2. When the same set of processed personal data is stored on several automatic or non-automatic media or when a hard copy of an automatic file also exists, notification of the existence of the file need be submitted only once.

Article 57. Files having more than one controller.

When a file is to be created for which several individuals or entities are to simultaneously act as controllers, each one of them must proceed to notify the competent authority of the creation of the respective file for registration in the General Data Protection Registry and, as appropriate, in file registries created by the regional supervisory authorities.

Article 58. Notification of file modification or deletion.

1. File entries must be kept current at all times. The Spanish Data Protection Agency or the regional supervisory authorities must be notified of any possible modification affecting the content of file registry entries for inclusion in the respective registry, pursuant to the provisions of Article 55.

2. When the controller decides to delete the file, the competent authorities must be notified of such decision for the purposes of cancelling the entry in the respective registry.

3. When a file controlled by a public authority is to be deleted or modified in a way affecting one of the requirements laid down in Article 55, the respective provision or decision must have been adopted in the terms provided in Chapter I of this title prior to notification of the modification or deletion.

Article 59. Notification forms and media.

1. The Spanish Data Protection Agency shall publish a resolution signed by its Director specifying the electronic forms to be used for notifying it of file creation, modification or deletion, either telematically or on hard copy. After consulting the regional data protection authorities, it shall also publish the forms for telematic submission of notification of public files by the regional supervisory authorities, pursuant to the provisions of Articles 55 and 58 of these regulations.

2. Notification forms may be downloaded cost-free from the Spanish Data Protection Agency's website.

3. The Spanish Data Protection Agency may establish simplified notification procedures depending on the circumstances surrounding processing or the type of files to which notification refers.

Article 60. File registration.

1. After conclusion of the procedures laid down in Title IX, Chapter IV, the Director of the Spanish Data Protection Agency, acting on a proposal by the General Data Protection Registry, shall issue a resolution authorising entry of the respective information in the registry, as appropriate.

2. The entry shall contain the code assigned by the registry, the identity of the controller and the file or processing operation, the description of its purpose and planned use, the processing system used in its organisation, as appropriate, the community of individuals whose data are to be obtained, the procedure for collecting the data, their origin, the data categories, the access service or unit and specification of the level of security measures required further to the provisions of Article 81.

The identity of the processor and file location, as well as the recipients of data surrendered or internationally transferred shall also be included, as appropriate.

Entries for public sector files shall also include a reference to the general provision creating or, as appropriate, modifying the file.

3. Registration of a file in the General Data Protection Registry does not exempt the controller from the rest of the obligations laid down in Constitutional Act 15/1999 of 13 December or other regulatory provisions.

Article 61. Cancellation of registration.

1. When, pursuant to the provisions of Article 58 of these regulations, the controller reports the deletion of a file, the Director of the Spanish Data Protection Agency shall issue a resolution determining cancellation of the respective entry after conclusion of the procedures established in Title IX, Chapter IV, Section One.

2. The Director of the Spanish Data Protection Agency may, in the exercise of his competencies, decide to cancel a file entry *ex officio* when circumstances are forthcoming that substantiate its non-existence after conclusion of the procedures laid down in Title IX, Chapter IV, Section Two of these regulations.

Article 62. Error correction.

The General Data Protection Registry may rectify material, factual or arithmetic errors in entries at any time, *ex officio* or upon request of the parties concerned, pursuant to the provisions of Article 105 of Act 30/1992 of 26 November.

Article 63. *Ex officio* entry of public sector files.

1. In exceptional circumstances, to guarantee data subjects' right to data protection and without prejudice to rules on mandatory notification, files may be registered in the General Data Protection Registry *ex officio*.

2. Publication of the provision or decision regulating the personal data files in the respective official journal further to the requirements laid down in Constitutional Act 15/1999 of 13 December shall be an indispensable requisite for applying the preceding provision.

3. The Director of the Spanish Data Protection Agency, acting on a proposal put forward by the General Data Protection Registry, may resolve to enter public sector files in the Registry and notify the controllers accordingly.

When the entry involves files subject to supervision by a supervisory authority in an autonomous community that has created its own file registry, said regional authority shall be notified thereof and may proceed to enter the file *ex officio*, as appropriate.

Article 64. Cooperation with regional supervisory authorities.

The Director of the Spanish Data Protection Agency may conclude partnering or cooperation agreements with the directors of the regional supervisory authorities where deemed suitable to ensure registration of the files subject to the competence of such regional authorities in the General Data Protection Registry.

TITLE VI

International data transfers

CHAPTER I

General provisions

Article 65. Compliance with the provisions of Constitutional Act 15/1999 of 13 December.

The provisions laid down in Constitutional Act 15/1999 of 13 December and these regulations shall apply without exception to all international data transfers.

Article 66. Authorisation and notification.

1. International data transfers shall only be regarded to conform to the provisions of Constitutional Act 15/1999 of 13 December and the present regulations where authorised by the Director of the Spanish Data Protection Agency. Such authorisation shall be granted when the exporter furnishes the guarantees referred to in Article 70 of these regulations.

The notification procedure shall be as established in Title IX, Chapter V, Section One of these regulations.

2. Authorisation shall not be required in the following circumstances.

a) When the State where the importer is located provides an adequate level of protection as defined in Chapter II of this title.

b) When the data are transferred under one of the circumstances described in Article 34, paragraphs a) to j) of Constitutional Act 15/1999 of 13 December.

3. All international data transfers must be duly notified and registered in the General Data Protection Registry pursuant to the procedure established in Title IX, Chapter IV, Section One of these regulations.

CHAPTER II

Transfers to states providing an adequate level of protection

Article 67. Adequate level of protection determined by the Spanish Data Protection Agency.

1. International data transfers shall not be subject to authorisation by the Director of the Spanish Data Protection Agency when the applicable provisions in the State where the importer is located afford an adequate level of protection in the opinion of the Director of the Spanish Data Protection Agency.

The suitability or otherwise of the level of protection afforded by the recipient country shall be evaluated on the grounds of all the circumstances surrounding the data transfer or category of data transfer. 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 industry-specific legal provisions in place in the third country in question, the content of the European Commission's reports and the professional standards and security measures in effect in such countries.

The resolutions issued by the Director of the Spanish Data Protection Agency determining that a given country has an adequate level of data protection shall be published in the *Official State Journal*.

2. The list of countries deemed to afford a comparable level of protection as per the provisions of the preceding paragraph shall be published by order of the Director of the Spanish Data Protection Agency.

This list shall be published and kept current via computerised or telematic methods.

Article 68. Adequate level of protection pursuant to a European Commission Decision.

International data transfers shall not be subject to authorisation by the Director of the Spanish Data Protection Agency when the importer is an individual or public or private entity located in a State declared by the European Commission to ensure a suitable level of protection.

Article 69. Temporary suspension of transfers.

1. In the cases set out in the preceding articles, the Director of the Spanish Data Protection Agency, in the exercise of the powers vested therein under Article 37.1 f) of Constitutional Act 15/1999 of 13 December, may, after hearing the exporter, determine the temporary suspension of data transfers to an importer located in a third State declared to have an adequate level of protection, in any of the following circumstances.

a) The data protection authority, or in the absence thereof, any other competent authority in the importing State, resolves that the importer has violated the data protection provisions established in his country's domestic law.

b) There is reasonable cause to believe that data protection rules or, as appropriate, principles, are being violated by the data importer, and the competent authorities in the State where the importer is located have not adopted or are not in the future going to adopt the necessary corrective measures, despite having been advised of the situation by the Spanish Data Protection Agency. In this case, data transfer may be suspended when its continuation might generate imminent risk of serious harm to data subjects.

2. Suspension shall be decided only after conclusion of the procedures established in Title IX, Chapter V, Section Two of these regulations.

In these cases, the European Commission shall be notified of the decision adopted by the Director of the Spanish Data Protection Agency.

CHAPTER III

Transfers to states that do not provide an adequate level of protection

Article 70. Transfers subject to authorisation from the Director of the Spanish Data Protection Agency.

1. When transfers are intended for a State that has not been declared to provide an adequate level of protection by the European Commission or the Director of the Spanish Data Protection Agency, authorisation must be obtained from the latter.

The notification procedure shall be as established in Title IX, Chapter V, Section One of these regulations.

2. Authorisation may be granted when the controller furnishes a written agreement concluded between the exporter and importer containing the necessary guarantees to the effect that protection of data subjects' private life and their fundamental rights and freedoms will be honoured and the exercise of their respective rights ensured.

To this end, agreements shall be regarded to establish suitable guarantees when concluded in accordance with European Commission Decisions 2001/497/EC of 15 June 2001, 2002/16/EC of 27 December 2001 and 2004/915/EC of 27 December 2004 or with the provisions of Commission decisions further to the stipulations laid down in Article 26.4 of Directive 95/46/EC.

3. In the case envisaged in the preceding paragraph, the Director of the Spanish Data Protection Agency may deny or, in the exercise of the power vested therein under Article **37.**1 f) of Constitutional Act 15/1999 of 13 December, temporarily suspend the transfer, after hearing the exporter, in any of the following circumstances.

a) When the degree of protection of the fundamental rights and public freedoms in the host country or its legislation are an impediment to guaranteeing full performance of the agreement and data subjects' exercise of the rights guaranteed therein.

b) When the recipient entity has previously failed to comply with the guarantees established in contractual clauses of this nature.

c) When there is reasonable cause to believe that the guarantees laid down in the agreement are not being or will not be honoured by the importer.

d) When there is reasonable cause to believe that the mechanisms for performance of the agreement are not or will not be effective.

e) When the transfer or continuation thereof, if already initiated, may create a situation detrimental to data subjects' interests.

Decisions on suspension of data transfers shall be subject to conclusion of the procedures established in Title IX, Chapter V, Section Two of these regulations.

Where required, the Commission of the European Communities shall be notified of resolutions adopted by the Director of the Spanish Data Protection Agency denying or suspending international data transfers for the causes referred to in this paragraph.

4. Authorisation for international data transfers may also be granted within multinational corporate groups when such groups have adopted internal standards or rules that constitute the necessary guarantees that data subjects' private lives and fundamental right to data protection will be protected, and where they also guarantee compliance with the principles laid down and the exercise of the rights acknowledged in Constitutional Act 15/1999 of 13 December and these regulations.

In such cases, the Spanish Data Protection Agency Director's authorisation shall only be forthcoming if the standards and rules are binding on group companies and enforceable under Spanish legislation.

Where authorisation is issued by the Director of the Spanish Data Protection Agency, both the agency and the subjects whose data are processed may demand compliance with the provisions of internal standards or rules at any time.

TITLE VII

Standard codes

Article 71. Object and nature.

1. The purpose of the standard codes referred to in Article 32 of Constitutional Act 15/1999 of 13 December is to adjust the provisions of that constitutional act and the present regulations to the peculiarities of processing operations conducted by the parties adhering to such codes.

To that end, they shall contain specific rules and standards with which to harmonise data processing effected by the parties concerned, facilitate the exercise of data subjects' rights and favour compliance with Constitutional Act 15/1999 of 13 December and the present regulations.

2. Standard codes shall constitute codes of conduct or good professional practice and shall be binding on the parties adhering thereto.

Article 72. Initiative and scope.

1. Standard codes shall be voluntary.

2. Industry codes may refer to all or part of the processing operations conducted by the entities engaging in a given industry, must be formulated by organisations representative of the industry at least in the geographic scope where they are to apply, and shall be without prejudice to the competency of such entities to adjust the code to their own particularities.

3. Standard codes instituted by a company must refer to all the processing conducted thereby.

4. Public authorities and public law corporations may adopt standard codes pursuant to the provisions of the legislation applicable thereto.

Article 73. Content.

1. Standard codes must be worded in clear and accessible language.

2. Standard codes must conform to the existing legislation and include at least the following items, defined with sufficient precision.

a) Clear and precise delimitation of the scope, the activities to which the code refers and the processing subject thereto.

b) Specific provisions on the application of data protection principles.

c) The establishment of uniform standards for the parties adhering to the code to ensure their compliance with the obligations laid down in Constitutional Act 15/1999 of 13 December.

d) The establishment of procedures that facilitate the exercise of data subjects' rights of access, rectification, erasure and objection.

e) The specification of any planned surrender or international transfer of data, specifying the guarantees that must be adopted.

f) Data protection training for individuals processing data, in particular as refers to their relationship with data subjects.

g) The supervisory mechanisms guaranteeing compliance with the provisions of the standard code by the parties adhering thereto in the terms laid down in Article 74 of these regulations.

3. In particular, the code must contain the following items.

a) Standard clauses for obtaining data subjects' consent to the processing or surrender of their data.

b) Standard clauses to inform data subjects that their data are being processed, when not obtained from them directly.

c) Forms for data subjects to exercise their rights of access, rectification, erasure and objection.

d) Model clauses for compliance with the formal requirements applicable to agreements with processors, as appropriate.

Article 74. Additional commitments.

1. Standard codes may include any other additional commitment assumed by the parties adhering thereto for more effective compliance with the existing data protection legislation.

2. They may also contain any other commitment established by the promoters, in particular as set out below.

a) The adoption of security measures over and above the requirements laid down in Constitutional Act 15/1999 of 13 December and these regulations.

b) The identification of categories of recipients or data importers.

c) Specific measures adopted geared to the protection of minors or certain communities of data subjects.

d) The establishment of a quality seal that identifies the parties adhering to the code.

Article 75. Guarantees of compliance with standard codes.

1. Standard codes must include independent supervisory procedures to guarantee compliance with the obligations assumed by the parties adhering thereto and establish a suitable system of penalties that constitutes an effective deterrent.

2. The procedure envisaged must guarantee the following.

a) The independence and impartiality of the supervisory body.

b) A simple, accessible, swift and cost-free method for submitting claims and complaints to that body relating to possible non-compliance with the standard code.

c) The principle of contradiction.

d) A scale for adjusting penalties to the severity of the non-compliance. Such penalties must act as deterrents and may entail suspension of adherence or expulsion of the entity involved. As appropriate, provision may be made for public disclosure of such penalties.

e) Obligation to notify the data subject of the decision adopted.

3. Moreover, and without prejudice to the provisions of Article 19 of Constitutional Act 15/1999 of 13 December, standard codes may include procedures for determining measures of restitution where harm is caused to data subjects as a result of failure to comply therewith.

4. The provisions of this article shall apply without prejudice to the competencies vested in the Spanish Data Protection Agency and, as appropriate, the regional supervisory authorities.

Article 76. List of adherents.

The standard code shall include a list of adherents in the annex, which must be kept current and made available to the Spanish Data Protection Agency.

Article 77. Deposit and public disclosure of standard codes.

1. In order for standard codes to attain such status further to Article 32 of Constitutional Act 15/1999 of 13 December and the present regulations, they must be deposited and registered with the Spanish Data Protection Agency's General Data Protection Registry or, as appropriate, with the registry created by autonomous communities, which shall forward them for inclusion in the General Data Protection Registry .

2. To this end, standard codes must be submitted to the respective supervisory authority and, where subject to a decision by the Spanish Data Protection Agency, the procedures for their registration shall be as laid down in Title IX, Chapter VI of these regulations.

3. The Spanish Data Protection Agency shall publicise all standard codes registered, preferably by computerised or telematic methods.

Article 78. Obligations subsequent to standard code registration.

After the code is published, its promoters or the bodies, individuals or entities so designated therein shall be bound to fulfil the following obligations.

a) Ensure public accessibility to current information on the promoters, the content of the standard code, the adherence and compliance procedures and the list of adherents referred to in the preceding article.

This information must be set out concisely and clearly and be permanently accessible via electronic systems.

b) Submit a yearly report to the Spanish Data Protection Agency on the activities conducted to publicise the existence of the standard code and further adherence thereto, the actions undertaken to verify compliance with the code and the results, the complaints and claims lodged and their handling and any other item the promoters deem worthy of mention.

When standard codes have been registered with a regional supervisory authority's registry, the report shall be submitted thereto, and forwarded thereby to the General Data Protection Registry.

c) Periodically assess the effectiveness of the standard code, measuring data subjects' satisfaction and, as appropriate, updating its content to adapt it to the general or industry-specific legislation on data protection in place at any given time.

Such assessment must be performed at least once every four years, except where the code commitments need to be adapted to amendments to the legislation in a shorter term.

d) To favour accessibility by all to the information on the standard code, with particular attention to people with disabilities or the elderly.

TITLE VIII

Security measures in personal data processing

CHAPTER I

General provisions

Article 79. Scope.

Controllers and processors must implement security measures pursuant to the provisions of this title, regardless of the processing system used.

Article 80. Security levels.

The security measures required of files and processing operations are divided into three levels: low, medium and high.

Article 81. Application of security levels.

1. Low level security measures must be in place in all personal data files and processing operations.

2. In addition to low level security measures, medium level measures must be in place in the following types of personal data files or processing operations.

a) Files or processing relating to the failure to comply with administrative obligations or the commission of misdemeanours or offences.

b) Files or processing whose operation is governed by Article 29 of Constitutional Act 15/1999 of 13 December.

c) Files or processing controlled by tax authorities and relating to the exercise of such authorities' tax-related powers.

d) Files or processing controlled by financial institutions and used for purposes relating to the provision of financial services.

e) Files or processing controlled by Social Security management agencies or bodies common to the entire Social Security system and related to the competencies thereof. Similarly, files or processing controlled by Social Security work accident and occupational disease mutual companies.

f) Files or processing containing a set of personal data that define citizens' characteristics or personalities and provide grounds for evaluating certain personality or behavioural traits.

3. In addition to low and medium level security measures, high level security must be in place in the following types of personal data files or processing.

a) Files or processing referring to ideology, trade union membership, religion, beliefs, racial origin, health or sex life.

b) Files or processing that refer to data obtained for law enforcement purposes without the data subjects' consent.

c) Files or processing involving gender violence-related data.

4. In addition to low and medium level security, the data on traffic and location contained in files whose controllers are public electronic communication service providers or that operate public electronic communications networks shall be subject to the high security requirements described in Article 103 of these Regulations.

5. Low level security measures shall suffice in files or processing involving data on ideology, trade union membership, religion, beliefs, racial origin, health or sex life under the following circumstances.

a) When the data are used solely to transfer money to the entities of which data subjects are members.

b) When such data are incidental or adventitious to the files or processing and bear no relation to their purpose.

6. Low level security measures may also be implemented in files or processing containing health-related data when they refer to the degree of disability or the mere determination of the data subject's disability or invalidity with a view to compliance with public obligations.

7. The measures included in each level described above are minimum requirements, without prejudice to specific laws or regulations in effect that may be applicable in each case or to measures adopted on the controller's own initiative.

8. For the purposes of facilitating compliance with the provisions of this title, when an information system contains files or involves processing that on the grounds of their specific purpose or use or the nature of the data contained therein, require a level of security measures different from the level in effect in the main system, they may be segregated from the latter. The respective level of security shall consequently be applicable to each case, providing the subjects' data and the users with access thereto can be delimited and note thereof is made in the security document.

Article 82. Processor.

1. When the controller facilitates access to data, the media on which they are saved or the information system resources where they are processed to a processor who provides his services in the former's premises, this circumstance must be specified in the controller's security document. The processor's staff must commit to complying with the security measures laid down in such document.

When such access is remote and the processor is not allowed to include such data in systems or media other than the controller's, the latter must specify this circumstance in his security document, and the processor's staff must commit to complying with the security measures laid down in the aforementioned document.

2. If the service is provided by a processor in his own premises, separate from the controller's premises, a security document must be drawn up in the terms established in Article 88 of these regulations, or any such existing document must be supplemented by identifying the file or processing operations and the controller and including the security measures to be implemented in respect of such operations.

3. Processor access to the data shall be subject to the security measures laid down in these regulations at all times.

Article 83. Services provided without access to personal data.

The controller shall adopt the necessary measures to restrict access to personal data, the media on which they are saved and information system resources by staff performing tasks that entail no personal data processing.

Where third party staff are involved, the agreement for provision of services shall explicitly prohibit their access to personal data and establish the secrecy obligations with respect to information that such staff may acquire during service provision.

Article 84. Proxies.

The competencies attributed to the controller in this title may be delegated to individuals designated for such purpose. The security document must specify the individuals vested with powers to grant such proxies and the

designated delegates. Such designation shall under no circumstances entail a delegation of the controller's responsibilities or liability.

Article 85. Data access through communications networks.

The security measures required for access to personal data through communications networks, public or otherwise, shall guarantee a level of security equivalent to the level called for in local access mode, pursuant to the criteria established in Article 80.

Article 86. Work performed outside the controller's or the processor's premises.

1. The storage of personal data on portable devices or processing outside the controller's or the processor's premises shall be subject to the controller's prior authorisation and the level of security corresponding to the type of file processed must be guaranteed at all times.

2. The authorisation referred to in the preceding paragraph must be specified in the security document and may be issued for a single user or a user profile, subject in either case to a specific validity period.

Article 87. Temporary files or working copies of documents.

1. Temporary files or copies of documents created solely to perform temporary or ancillary tasks must meet the security level assigned thereto further to the criteria laid down in Article 81.

2. Any temporary file or working copy so created shall be erased or destroyed when no longer needed for the purposes for which it was created.

CHAPTER II

The security document

Article 88. The security document.

1. The controller shall draw up a security document that shall include the technical and organisational measures to be required of personnel with access to information systems, in keeping with the existing legislation on security.

2. All files and processing operations may be included in a single security document, or a separate document may be formulated for each file or processing operation. Several security documents may also be drawn up in which files or processing operations are grouped by the processing system used in their organisation or any other criterion defined by the controller. All security documents are internal instruments.

3. The document must contain at least the following items.

a) Scope, with a detailed specification of the resources protected.

b) Measures, norms, procedures, rules and standards geared to guaranteeing the level of security required in these regulations.

c) Staff duties and obligations with respect to the processing of the personal data included in the files.

d) Personal data file structure and description of the information systems by which they are processed.

e) Procedures for notification and handling of incidents and response thereto.

f) Data back-up and retrieval procedures for automatic files or automatic processing.

g) Measures required for transporting, destroying or, as appropriate, reusing media and documents.

4. Where medium or high security level measures described in this title are applicable to the files, the security document must also contain the following items.

a) The identity of the controller or controllers.

b) The periodic control operations to be conducted to verify compliance with all the provisions of the document itself.

5. When data are processed for third parties, the security document must identify the files processed or processing operations performed by the processor, with explicit reference to the agreement or document regulating the conditions of the work commissioned, as well as the identity of the controller and validity period of the commission.

6. Where the personal data in a file or processing operation are uploaded to and processed exclusively in the processor's systems, the controller shall make note thereof in the security document. When all or part of the controller's files or processing operations are so affected, the responsibility for keeping the security document may be delegated to the processor, with the exception of matters relating to data contained in the controller's own resources. This fact shall be explicitly reflected in the agreement concluded under the terms of Article 12 of Constitutional Act 15/1999 of 13 December, and the files or processing operations involved shall be specified therein.

In such cases, the processor's security document shall be the basis for determining compliance with the provisions of these regulations.

7. The security document must be kept current at all times and shall be revised whenever any relevant changes are made to the information system, the processing system used, the organisation thereof, the content of the information included in the files or processing operations or, as appropriate, when relevant changes are made as a result of the periodic control operations conducted. A change shall be understood to be relevant when it may impact compliance with the security measures in place.

8. The content of the security document shall be in keeping at all times with the personal data security legislation in effect.

CHAPTER III

Security measures applicable to automatic files and processing

SECTION 1. LOW LEVEL SECURITY MEASURES

Article 89. Staff duties and obligations.

1. The duties and obligations of each user or user profile with access to personal data and information systems shall be clearly defined and documented in the security document.

The control functions or authorisations delegated by the controller shall likewise be defined.

2. The controller shall adopt the necessary measures to ensure that the staff is provided comprehensible information on the security measures applicable to the performance of their duties and the possible consequences of failure to comply therewith.

Article 90. Incident records.

A procedure must be in place to notify and handle incidents affecting personal data and establish a registry for recording the type of incident, when it arose or, as appropriate, was detected, the person who reported the incident and to whom it was reported, the effects thereof and the corrective measures applied.

Article 91. Access control.

1. Users shall have access only to the resources required to perform their duties.

2. The controller shall formulate and keep a current list of users and user profiles and the type of access authorised for each.

3. The controller shall establish mechanisms to prevent users from accessing resources other than as authorised.

4. Only the staff authorised to do so in the security document may grant, alter or cancel authorised access to resources, further to the criteria established by the controller.

5. When outside personnel has access to the resources, they must be subject to the same security conditions and obligations as the controller's own staff.

Article 92. Media and document management.

1. The media and documents containing personal data must identify the type of information contained, be inventoried and be accessible only to authorised staff as specified in the security document.

Such obligations shall not be required where the physical characteristics of the medium prevent compliance therewith, although this circumstance shall be recorded in the security document.

2. Transmission of media or documents containing personal data outside the premises under the controller's supervision, including transmission by electronic mail or as attachments thereto, must be authorised by the controller or duly authorised in the security document.

3. Measures shall be adopted to prevent theft or loss of or undue access to information while in transit.

4. Whenever any document or medium containing personal data is to be discarded, it must first be destroyed or erased via the adoption of measures geared to preventing access to or retrieval of the information contained thereon.

5. Media containing personal data deemed by the organisation to be particularly sensitive may be identified with labelling systems comprehensible and meaningful to users with authorised access to such media and documents, but which hinder identification by anyone not so authorised.

Article 93. Identification and authentication.

1. The controller must adopt measures to guarantee correct user identification and authentication.

2. The controller shall establish a mechanism to unequivocally and individually identify any user attempting to access the information system and verify his authorisation to do so.

3. When the authentication mechanism is based on the existence of passwords, an assignment, distribution and storage system must be in place to guarantee their confidentiality and security.

4. The security document shall establish the periodicity, which may not be over one year, with which the passwords must be changed. While in effect, such passwords shall be stored in an unintelligible manner.

Article 94. Back-up copies and recovery.

1. Procedures must be established for making back-up copies at least weekly, except where the data are not updated in that period of time.

2. Recovery procedures shall likewise be established to guarantee data reconstruction to the condition prevailing prior to loss or destruction.

Data shall be saved manually only where loss or destruction might affect partially automatic files or processing operations, and only where the existence of such documents could be used to attain the objective referred to in the preceding paragraph. This fact must be recorded and justified in the security document.

3. Every six months, the controller shall verify the definition, operation and application of data back-up and recovery procedures, to ensure they are satisfactory.

4. Trials run prior to the implementation or modification of information systems that process personal data shall not be conducted with real data unless the security level for the processing conducted is ensured and the performance of such trials is recorded in the security document.

Where trials with real data are planned, a back-up copy must be made prior thereto.

SECTION 2. MEDIUM LEVEL SECURITY MEASURES

Article 95. Security manager.

The security document must designate one or several security managers responsible for coordinating and monitoring the measures defined in such document. Managers may be designated with responsibility for all personal data files or processing operations, or separate managers may be designated for different processing systems. These circumstances must be clearly specified in the security document.

The designation of security managers shall release neither the controller nor the processor from any liability or responsibility incumbent thereon under these regulations.

Article 96. Audit.

1. Information systems and data processing and storage facilities subject to medium or higher security levels shall be audited internally or externally in no less than two-year intervals to verify compliance with the present title.

Exceptional audits must be conducted whenever substantial modifications are made to the information system that may impact compliance with the security measures implemented, to verify the adaptation, suitability and effectiveness of such changes. The two-year interval specified in the preceding paragraph shall be counted from the date of each new audit.

2. The auditor's report must express an opinion on the conformity or otherwise of the measures and controls in place to the act and related regulations, identify any shortcomings and propose any necessary corrective or supplementary measures. It shall also contain the data, facts and observations serving as a basis for the opinions expressed and recommendations proposed.

3. Auditors' reports shall be analysed by the competent security manager, who shall refer the conclusions to the controller to adopt any suitable corrective measures. These reports shall also be made available to the Spanish Data Protection Agency or the regional supervisory authorities, as appropriate.

Article 97. Media and document management.

1. A system must be established for recording incoming media that directly or indirectly identifies the type of document or medium, date and time, sender, number of documents or media received, type of information contained, transmission method and duly authorised person responsible for acceptance thereof.

2. A system must likewise be established for recording outgoing media that directly or indirectly identifies the type of document or medium, date and time, recipient, number of documents or media sent, type of information contained, transmission method and duly authorised person responsible therefor.

Article 98. Identification and authentication.

The controller shall establish a mechanism that limits the number of repeated unauthorised attempts to access the information system.

Article 99. Physical access control.

Only the staff authorised in the security document may access the premises where the hardware supporting the information systems is installed.

Article 100. Incident records.

1. The registry regulated in Article 90 shall also contain the procedures undertaken to recover data, identifying the person running the process, the data restored and, as appropriate, any data having to be manually saved in the recovery process.

2. The implementation of data recovery procedures shall be subject to controller authorisation.

SECTION 3. HIGH LEVEL SECURITY MEASURES

Article 101. Media management and distribution.

1. Media shall be identified with labelling systems comprehensible and meaningful to users with authorised access to such media and documents, but which hinder identification by anyone not so authorised.

2. Prior to media distribution, any personal data thereon shall be encrypted or otherwise altered to guarantee that the information is not accessible or liable to manipulations while in transit.

The data in portable devices shall also be encrypted when such devices are removed from the premises under the controller's supervision.

3. Personal data processing in portable devices not accommodating data encryption should be avoided. Where strictly necessary, such circumstance shall be recorded and justified in the security document and measures shall be adopted to counter the risks of processing data in unprotected environments.

Article 102. Back-up copies and recovery.

A back-up copy of the data and of the data recovery procedures shall be kept in a place other than where the computer hardware in which they are processed are located. Such place must comply with the security requirements laid down in this title or the elements used must guarantee information integrity and recovery in a manner ensuring that the data can be recovered.

Article 103. Access records.

1. Each attempted access shall be the object of a record identifying the user, the date and time of the attempt, the file accessed, the type of access and whether it was authorised or denied.

2. Where access was authorised, information identifying the record accessed must also be saved.

3. The mechanisms governing access records shall be under the direct supervision of the competent security manager and shall prevent inactivation or manipulation of such records.

4. Data so recorded must be stored for at least two years.

5. The controller shall review the control information recorded at least once a month and shall formulate a report on the reviews conducted and any problems detected.

6. Access recording as defined in this article shall not be required where both of the following conditions are met.

a) The controller is a natural person.

b) The controller guarantees that only he accesses and processes personal data.

The concurrent existence of the two circumstances referred to in the preceding paragraph must be explicitly recorded in the security document.

Article 104. Telecommunications.

When high level security measures must be implemented further to Article 81.3, prior to transmission across public or wireless electronic communication networks, personal data shall be encrypted or otherwise altered to ensure that the information is not intelligible to or liable to manipulation by third parties.

CHAPTER IV

Security measures applicable to non-automatic files and processing

SECTION 1. LOW LEVEL SECURITY MEASURES

Article 105. Obligations in common with automatic files and processing.

1. In addition to the provisions of the present chapter, non-automatic files shall be subject to the stipulations laid down in Chapters I and II of the present title with regard to:

a) scope;

b) security levels;

c) processor;

d) services provided not requiring access to personal data;

e) proxies;

f) work performed outside the controller's or the processor's premises;

g) working copies of documents;

h) security document.

2. The provisions of Chapter III, Section One of the present title shall also be applicable as regards:

a) staff duties and obligations;

b) incident records;

c) access control;

d) media management.

Article 106. Filing criteria.

Media or documents shall be filed in accordance with the criteria set out in the respective legislation. Such criteria must ensure that documents are duly conserved and readily located and consulted and that they guarantee as well the exercise of the rights of objection to processing, access, rectification and erasure.

Where no applicable legislation is in place, the controller must establish the file criteria and procedures to be followed.

Article 107. Storage devices.

The storage devices for documents containing personal data must be fitted with mechanisms that obstruct opening. When the physical characteristics of such devices rule out the foregoing, the controller shall adopt measures that prevent access by unauthorised persons.

Article 108. Media custody.

While documents containing personal data are in use for revision or other handling, before or after being filed, and consequently are not in the storage devices described in the preceding paragraph, the person in charge thereof must custody such documents and prevent access by unauthorised persons at all times.

SECTION 2. MEDIUM LEVEL SECURITY MEASURES

Article 109. Security manager.

One or several security managers shall be designated to perform the duties laid down in Article 95 of these regulations, under the terms thereof.

Article 110. Audit.

The files to which the present section is applicable shall be internally or externally audited at intervals of no more than two years to verify compliance with the provisions of the present title.

SECTION 3. HIGH LEVEL SECURITY MEASURES

Article 111. Information storage.

1. The filing cabinets, folders or other non-automatic elements for storing non-automatic personal data files must be kept in areas where access is protected by doors fitted with locks or similar devices. These areas must remain locked when the documents filed therein are not needed.

2. If the controller's premises are unable to comply with the provisions of the preceding paragraph, the controller shall adopt alternative measures which shall be recorded and duly justified in the security document.

Article 112. Copy or reproduction.

1. Documents may only be copied or reproduced under the supervision of the authorised staff listed in the security document.

2. Discarded copies or reproductions must be destroyed in a way that prevents access to the information contained therein or its subsequent retrieval.

Article 113. Access to documents.

1. Access to documents shall be limited exclusively to authorised personnel.

2. Mechanisms shall be established to identify access details where documents are accessible to several users.

3. Access by persons not included in the preceding paragraph must be duly recorded pursuant to the procedure established for this purpose in the security document.

Article 114. Relocation of documents.

Whenever documents contained in a folder are to be physically moved, measures must be adopted to prevent access to or manipulation of the information contained therein.

TITLE IX

Spanish Data Protection Agency procedures

CHAPTER I

General provisions

Article 115. Applicable legislation.

1. The procedures conducted by the Spanish Data Protection Agency shall be governed by the provisions of the present title, and subsidiarily by the stipulations laid down in Act 30/1992 of 26 November on the Legal Framework for Public Authorities and General Administrative Procedures.

2. Specifically, the provisions regulating general administrative procedures shall be applicable to representation before the agency in respect of its procedures.

Article 116. Public disclosure of resolutions.

1. The Spanish Data Protection Agency shall make its resolutions public, with the exception of resolutions regarding the entry of files or processing operations in the General Data Protection Registry or the registration therein of standard codes, where such procedures were initiated prior to 1 January 2004 or refer to the dismissal of inspection proceedings instituted after such date.

2. Resolutions shall be published within one month of the date of notification of the parties concerned, preferably on the Spanish Data Protection Agency's website.

3. In such notifications, the parties concerned shall be explicitly informed of the public disclosure of resolutions pursuant to Article **37.**2 of Constitutional Act 15/1999 of 13 December.

4. Publication shall be subject to the personal data decoupling criteria established by a resolution issued by the agency's Director in this regard.

CHAPTER II

Protection procedures for the rights of objection, access, rectification and erasure

Article 117. Claim proceedings.

1. Proceedings shall be instituted at the request of a data subject or subjects, who must clearly express the content of their claim and the provisions of Constitutional Act 15/1999 of 13 December that they deem have been violated.

2. Claims received by the Spanish Data Protection Agency shall be forwarded to the controller for the purposes of submission thereby of any relevant allegations, which must be received within fifteen days.

3. Upon receipt of the allegations or lapsing of the aforementioned term, the Spanish Data Protection Agency shall examine the reports, evidence and other relevant items, hear the data subject and again the controller, and issue a resolution on the claim lodged.

Article 118. Duration of proceedings and effects of lack of an explicit resolution.

1. In protection of rights proceedings, a resolution must be delivered and notice thereof served within no more than six months counting from the date when the data subject's or subjects' claim was lodged with the Spanish Data Protection Agency.

2. If no explicit resolution is forthcoming or notice served within that period, the data subject may regard his claim to have been endorsed under the principle of "silence means consent".

Article 119. Enforcement of the resolution.

If the resolution in protection of rights cases is favourable to the claimant, the controller shall be required to submit to the rights of the data subject constituting the object of the claim within ten days of the notification and to confirm compliance therewith in a written report submitted to the Spanish Data Protection Agency within the same term.

CHAPTER III

Procedures relating to the exercise of the power to impose penalties

SECTION 1. GENERAL PROVISIONS

Article 120. Scope.

1. The provisions contained in the present chapter shall be applicable to procedures relating to the Spanish Data Protection Agency's exercise of its power to impose penalties, attributed thereto under Constitutional Act 15/1999 of 13 December on Personal Data Protection, Act 34/2002 of 11 July on Information Society and Electronic Commerce Services and General Act 32/2003 of 3 November on Telecommunications.

2. That notwithstanding, the provisions of Article 121 in Section Four of this chapter shall only be applicable to procedures referring to the exercise of the power to impose penalties laid down in Constitutional Act 15/1999 of 13 December.

Article 121. Immobilisation of files.

1. In the event of a very serious infringement as defined in Constitutional Act 15/1999 of 13 December, consisting of the illegal use or surrender of personal data that constitutes an attempt against the exercise of citizens' rights and the free development of their personality guaranteed by the Constitution and the law or the serious obstruction of the exercise of such rights, the Director of the Spanish Data Protection Agency may, at any stage of the proceedings, require the controllers of private or public sector personal data files to cease their illegal use or surrender thereof.

2. This notice must be heeded within three days, which shall not be extendible, during which the controller may formulate any allegations deemed pertinent to possible lifting of the measure.

3. If the notice goes unheeded, the Data Protection Agency may, subject to a duly justified resolution, immobilise such files or processing operations for the sole purpose of restoring the data subjects' rights.

SECTION 2. PRELIMINARY REVIEW

Article 122. Institution.

1. Before penalisation proceedings are initiated, a preliminary review may be conducted to determine whether the circumstances warrant such proceedings. In particular, this review shall be geared to determining as precisely as possible any facts that might justify the institution of proceedings, identifying the person or body who may be responsible and establishing any circumstances relevant to the case.

2. The preliminary review shall be conducted *ex officio* by the Spanish Data Protection Agency either on its own initiative or as a result of a complaint or justified request submitted by another body.

3. When the review is conducted as a result of a complaint or justified request from another body, the Spanish Data Protection Agency shall acknowledge receipt of the claim or request and may call for any document it deems suitable to verify the facts that may justify the institution of penalisation proceedings.

4. This preliminary review shall not last for over twelve months from the date the complaint or justified request referred to in paragraph 2 was received at the Spanish Data Protection Agency or, if no report or request is involved, from the data the Agency Director initiated the review process.

If no penalisation proceedings are instituted or notice served within the aforementioned period, the preliminary review shall expire.

Article 123. Personnel qualified to conduct preliminary reviews.

1. Preliminary reviews shall be conducted by the data inspection staff qualified to perform inspection duties.

2. (Cancelled).

3. Officials conducting the inspections referred to in the two preceding paragraphs shall be regarded to be public authorities in the performance of their duties.

They shall be required to honour the confidentiality of the information of which they become aware in the exercise of such duties, even after separation therefrom.

Article 124. Obtaining information.

Inspectors may request any information they require to perform their duties. To that end they may request that documents and data be displayed or submitted and examine them where they are deposited; obtain copies thereof; inspect hardware and software; request that processes, programs or file management and support procedures be run for the files under investigation; and gain access to the places where they are installed.

Article 125. In situ action.

1. The preliminary review may entail inspection visits by the designated inspectors at the inspected party's premises or headquarters or where the files are located, as appropriate. The inspectors shall be granted prior authorisation in this regard by the Director of the Spanish Data Protection Agency.

Inspections may be conducted at the inspected party's registered office, headquarters, specifically related premises or any other of the latter's premises, including premises where processing is performed by a processor.

Authorisation need only specify the identity of the individual or body inspected and stipulate that the authorised inspector is duly qualified.

2. Where inspections are conducted as envisaged in the preceding paragraph, they shall conclude with the formulation of a report reflecting the action undertaken during the inspection visit or visits.

3. The report, which shall be issued in duplicate, shall be signed by the inspectors involved and the party inspected, who may include therein any allegations or remarks he deems suitable.

Where the party inspected refuses to sign the report, this circumstance shall be explicitly recorded therein. In any event, the inspected party's signature shall signify not his agreement with the report, but merely acknowledgement of his receipt thereof.

The party inspected shall be furnished with one of the two originals of the inspection report, while the other shall be included in the dossier.

Article 126. Result of the preliminary review.

1. Upon conclusion, the preliminary review shall be submitted to the Director of the Spanish Data Protection Agency for a decision.

If the facts stemming from the review fail to justify charges for any infringement whatsoever, the Director of the Spanish Data Protection Agency shall deliver a resolution to dismiss the case and notify the party inspected accordingly, as well as the party lodging the charges, as appropriate.

2. If signs of an infringement are perceived, the Director of the Spanish Data Protection Agency shall determine the institution of penalisation proceedings, or infringement proceedings where public authorities are involved, which shall be handled in accordance with Sections Three and Four of the present chapter, respectively.

SECTION 3. PENALISATION PROCEDURE

Article 127. Institution of proceedings.

The decision to institute penalisation proceedings must specifically contain the following items.

a) dentity of the presumably responsible individual or individuals.

b) Succinct description of the charges, their possible category and the respective penalties, without prejudice to the result of the investigation.

c) Indication that the competent authority for delivering a resolution is the Director of the Spanish Data Protection Agency.

d) Notice advising the individual presumably responsible that he can acknowledge his responsibility voluntarily, in which case a resolution shall be issued directly.

e) Designation of a case officer and secretary, as appropriate, explicitly specifying the system for challenging their designation.

f) Explicit indication of the controller's right to formulate allegations, be heard in the proceedings and put forward any evidence he deems suitable.

g) Provisional measures that may be determined, further to the provisions of Section One of this chapter.

Article 128. Maximum term for resolutions.

1. The term for delivering a resolution shall be as laid down in the provisions applicable to each penalisation procedure and shall be counted from the date institution is ordered until the date notice of the resolution is served or the date when a duly substantiated attempt to do so is made.

2. If the term lapses before an explicit resolution is delivered and notice thereof served, the proceedings shall expire and the charges shall be dismissed.

SECTION 4. PROCEDURES FOR DECLARING PUBLIC AUTHORITY INFRINGEMENT OF CONSTITUTIONAL ACT 15/1999 OF 13 DECEMBER

Article 129. General provision.

The procedure for declaring the existence of an infringement of Constitutional Act 15/1999 of 13 December committed by public authorities shall be as established in Section Three of this chapter.

CHAPTER IV

Procedures relating to file registration or cancellation

SECTION 1. PROCEDURE FOR REGISTERING FILE CREATION, MODIFICATION OR DELETION

Article 130. Initiation of the procedure.

1. The procedure shall be initiated as the result of the notification of the creation, modification or deletion of a file by the party concerned, or, as appropriate, of a referral from the regional supervisory authorities described in the present regulations.

2. The notification shall be effected by completing the electronic forms published for that purpose by the Spanish Data Protection Agency further to the provisions of Article 59, paragraph 1 of these regulations.

When the notification refers to the modification or deletion of a file, the registration code under which the file is entered in the General Data Protection Registry must be specified.

3. Notifications shall be sent electronically, either on-line over an electronic signature or on computer media, using the cost-free program for generating notifications provided by the Agency.

Hard copy notifications shall likewise be valid when furnished on the forms published by the Agency.

4. The controller must specify an address for notifications during the procedure.

Article 131. Particularities in the notification of public sector files.

1. Notifications relating to public sector files shall include a copy of the provision or decision whereby they were created, modified or deleted, referred to in Article 52 of the present regulations.

When the official journal publishing said provision or decision is Internet-accessible, the notification need only specify the respective URL.

2. If the notification received lacks the necessary information or contains formal defects, the General Data Protection Registry shall call upon the controller to complete or rectify the notification. The term for correcting or improving the application for registration shall be three months if it entails amending the provision or decision on file creation.

Article 132. Decision on registration or cancellation.

If the notification on file creation, modification or deletion contains the necessary information and meets all other legal requirements, the Director of the Spanish Data Protection Agency, acting on a proposal by the General Data Protection Registry, shall decide, respectively, to register the file and assign it a registration code, modify the file entry or proceed to its cancellation.

Article 133. Inadmissibility or denial of registration.

The Director of the Spanish Data Protection Agency, acting on a proposal by the General Data Protection Registry, shall deliver a resolution denying registration, modification or cancellation when, further to the documents furnished by the controller, the notification is not in accordance with the provisions of Constitutional Act 15/1999 of 13 December.

The resolution shall be duly justified and explicitly list the reasons why registration, modification or cancellation cannot be effected.

Article 134. Duration of proceedings and effects of lack of an explicit resolution.

1. The term for delivering a resolution on registration, modification or cancellation and serving notice thereof shall be one month.

2. If no explicit resolution is delivered or notice served within that term, the file shall be regarded to be registered, modified or cancelled for all intents and purposes.

SECTION 2. PROCEDURE FOR EX OFFICIO CANCELLATION OF REGISTERED FILES

Article 135. Initiation of the procedure.

Ex officio cancellation procedures for files registered in the General Data Protection Registry must be initiated by a decision of the Director of the Spanish Data Protection Agency, either on the Agency's own initiative or by virtue of a complaint.

Article 136. Case conclusion.

The resolution, after hearing the party concerned, shall determine whether file cancellation is in order or otherwise.

If the resolution determines that the file should be cancelled, it shall be forwarded to the General Data Protection Registry to proceed thereto.

CHAPTER V

Procedures relating to international data transfers

SECTION 1. PROCEDURE FOR AUTHORISING INTERNATIONAL DATA TRANSFERS

Article 137. Initiation of the procedure.

1. The procedure for obtaining authorisation for international data transfers to third countries referred to in Article 33 of Constitutional Act 15/1999 of 13 December and Article 70 of these regulations must be initiated by the exporter who plans to effect the transfer.

2. In his application, in addition to legal requirements, the exporter shall specify the following items.

a) Identity of the file or files containing the data to be internationally transferred, specifying their denomination and the code under which the file is registered in the General Data Protection Registry.

b) The transfer or transfers for which authorisation is requested, specifying the purpose justifying such action.

c) The documents substantiating the guarantees required to obtain authorisation as well as compliance with the necessary legal requirements to effect the transfer, as appropriate.

When authorisation is based on a contract between the data exporter and importer, a copy thereof must be furnished and sufficient power of attorney of the parties concluding the contract must be duly substantiated.

If the application for authorisation is based on the existence of the arrangements set out in Article 70, paragraph 4, the data processing standards or rules adopted by the group must be provided, as well as documents substantiating that they are binding and effective within the group. Documents shall also be furnished substantiating data subjects' or the Spanish Data Protection Agency's capacity to claim liability if harm is caused to data subjects or data protection standards are violated by importers.

Article 138. Public inquiry.

1. When, pursuant to the provisions of Article 86.1 of Act 30/1992 of 26 November, the Director of the Spanish Data Protection Agency decides to establish a public inquiry, the term for the submission of allegations shall be ten days from the date of publication of the announcement in the *Official State Journal*, as provided for in such act.

2. Access shall not be allowed to the information in dossiers involving the circumstances laid down in Article 37.5 of Act 30/1992 of 26 November.

3. Where allegations are submitted within the term established in paragraph 1, they shall be forwarded to the applicant requesting authorisation, who may raise any counter-allegations he deems fitting within ten days.

Article 139. Acts subsequent to the resolution.

1. When the Director of the Spanish Data Protection Agency resolves to authorise an international data transfer, such authorisation shall be forwarded to the General Data Protection Registry for registration thereof.

The General Data Protection Registry shall register the authorisation for the international transfer *ex officio*.

2. Authorisation for or denial of the international data transfer shall be forwarded to the Ministry of Justice, which shall proceed to notify the other European Union States and the European Commission thereof pursuant to the provisions of Article 26.3 of Directive 95/46/EC.

Article 140. Duration of proceedings and effects of lack of an explicit resolution.

1. A resolution must be delivered and notice thereof served within three months, counting from the date of receipt of the application by the Spanish Data Protection Agency.

2. If no explicit resolution is delivered or notice served, the international data transfer shall be understood to be authorised.

SECTION 2. PROCEDURE FOR THE TEMPORARY SUSPENSION OF INTERNATIONAL DATA TRANSFERS

Article 141. Institution.

1. In the circumstances envisaged in Article 69 and Article 70, paragraph 3, the Director of the Spanish Data Protection Agency may decide to temporarily suspend an international data transfer.

2. In such cases, the Director shall issue a decision to institute proceedings for temporary suspension of the transfer. The decision must be justified and based on the circumstances laid down in these regulations.

Article 142. Examination and resolution.

1. The decision shall be forwarded to the exporter, who shall have fifteen days in which to defend his rights.

2. After the allegations are received or the term lapses, the Director shall deliver his resolution and determine the temporary suspension of the international data transfer, as appropriate.

Article 143. Acts subsequent to the resolution.

1. The Director of the Spanish Data Protection Agency shall forward the resolution to the General Data Protection Registry for entry therein.

The General Data Protection Registry shall register the temporary suspension of the international transfer *ex officio*.

2. The resolution shall be forwarded to the Ministry of Justice, which shall proceed to notify the other European Union States and the European Commission thereof pursuant to the provisions of Article 26.3 of Directive 95/46/EC.

Article 144. Lifting of the temporary suspension.

1. The suspension shall be lifted as soon as the causes warranting the measure cease to exist, under a resolution delivered by the Director of the Spanish Data Protection Agency, which shall be forwarded to the exporter.

2. The Director of the Spanish Data Protection Agency shall forward the resolution to the General Data Protection Registry for entry therein.

The General Data Protection Registry shall register the authorisation to lift the temporary suspension of the international transfer *ex officio*.

3. The resolution shall be forwarded to the exporter and the Ministry of Justice, which shall proceed to notify the other European Union States and the European Commission thereof pursuant to the provisions of Article 26.3 of Directive 95/46/EC.

CHAPTER VI

Procedure for registration of standard codes

Article 145. Initiation of the procedure.

1. The procedure for registration of standard codes in the General Data Protection Registry must be initiated by the entity, body or association promoting the standard code.

2. The application, which must meet all legally established requirements, shall be submitted with the following documents.

a) Substantiation of the representation vested in the individual submitting the request.

b) Content of the agreement, convention or decision adopted in the respective scope, approving the standard code submitted.

c) Where the standard code is the result of an industry-wide agreement or company decision, certification of its adoption and legitimisation of the body that adopted it.

d) In the circumstance envisaged in the preceding sub-paragraph, copy of the by-laws of the association, industry organisation or entity under which the code was approved.

e) For standard codes submitted by industry associations or organisations, documents relating to their representativeness in the industry.

f) For standard codes based on company decisions, a description of the processing operations to which the standard code refers.

g) Standard code submitted to the Spanish Data Protection Agency.

Article 146. Analysis of the substantive aspects of standard codes.

1. In the thirty days following the notification or submission of the correction of defects, the General Data Protection Registry may convene a meeting with the parties concerned to clarify matters or details relating to the substantive content of the standard code.

2. After the above term lapses, the General Data Protection Registry shall deliver a report on the characteristics of the draft standard code.

3. The documents presented and the Registry's report shall be referred to the Legal Advisory Board, which shall determine whether the code complies with the requirements laid down in Title VII of these regulations.

Article 147. Public inquiry.

1. When, pursuant to the provisions of Article 86.1 of Act 30/1992 of 26 November, the Director of the Spanish Data Protection Agency decides to establish a public inquiry, the term for the submission of allegations shall be ten days from the date of publication of the announcement in the *Official State Journal*, as provided for in such act.

2. Access shall not be allowed to the information in dossiers involving the circumstances laid down in Article 37.5 of Act 30/1992 of 26 November.

Article 148. Improvements to the standard code.

If further documents or amendments to the standard code submitted need to be furnished during the proceedings, the Spanish Data Protection Agency may call upon the applicant to introduce the necessary amendments within thirty days and re-submit the resulting text to the Spanish Data Protection Agency.

If the applicant fails to furnish the information required, the proceedings shall be suspended.

Article 149. Hearings.

If allegations are submitted during the proceedings provided for in Article 148, they shall be forwarded to the applicant, who may raise any counter-allegations he deems fitting within ten days.

Article 150. Resolution.

1. Once the requirements established in the preceding articles are met, the agency's Director shall decide whether registration of the standard code in the General Data Protection Registry is in order or otherwise.

2. When the Director of the Spanish Data Protection Agency resolves to authorise registration of a standard code, such authorisation shall be forwarded to the General Data Protection Registry for registration thereof.

Article 151. Duration of proceedings and effects of lack of an explicit resolution.

1. A resolution must be delivered and notice thereof served within six months counting from the date of receipt of the application by the Spanish Data Protection Agency.

2. If no explicit resolution is delivered or notice thereof served within the above term, the applicant shall regard his application to be approved.

Article 152. Public disclosure of standard codes by the Spanish Data Protection Agency.

The Spanish Data Protection Agency shall publicly disclose the content of the standard codes registered in the General Data Protection Registry, preferably by electronic or telematic methods.

CHAPTER VII

Other procedures handled by the Spanish Data Protection Agency

SECTION 1. PROCEDURE FOR EXEMPTION FROM THE DUTY OF INFORMATION

Article 153. Initiation of the procedure.

1. The procedure to obtain exemption from the Spanish Data Protection Agency from the obligation to inform data subjects of the processing of their personal data when such action is impossible or calls for an inordinate effort, as provided in Article 5, paragraph 5 of Constitutional Act 15/1999 of 13 December, must be initiated by the controller seeking exemption.

2. In his application, in addition to meeting the requirements laid down in Article 70 of Act 30/1992 of 26 November, the controller must proceed as follows.

a) Clearly identify the data processing operation for which exemption from the duty of information is sought.

b) Explicitly describe the reasons why compliance with the duty of information is impossible or would call for an inordinate effort.

c) Provide a detailed explanation of the compensatory measures proposed in the event of exemption from the duty of information.

d) Furnish an informational clause whose dissemination in the terms specified in the request would compensate for the exemption from the duty of information.

Article 154. Proposal for new compensatory measures.

1. If the Spanish Data Protection Agency considers the compensatory measures proposed by the applicant to be insufficient, it may require the adoption of measures to supplement or replace the measures proposed in his application.

2. The decision shall be forwarded to the applicant, who shall have fifteen days in which to defend his rights.

Article 155. Conclusion of the procedure.

Once the proceedings described in the preceding articles are concluded, the Director of the Spanish Data Protection Agency shall deliver a resolution, granting or denying exemption from the duty of information. The resolution may impose the adoption of the supplementary measures referred to in the preceding paragraph.

Article 156. Duration of proceedings and effects of lack of an explicit resolution.

1.A resolution must be delivered and notice thereof served within six months counting from the date of receipt of the controller's request by the Spanish Data Protection Agency.

2. If no explicit resolution is forthcoming or notice served within that term, the party concerned may regard his application to have been approved under the principle of "silence means consent".

SECTION 2. PROCEDURE FOR AUTHORISING DATA CONSERVATION FOR HISTORIC, STATISTICAL OR SCIENTIFIC PURPOSES

Article 157. Initiation of the procedure.

1. The procedure for obtaining official acknowledgement from the Spanish Data Protection Agency of the existence of data with historic, scientific or statistical value in a given processing operation for the intents and purposes set out in Constitutional Act 15/1999 of 13 December and the present regulations must be initiated by the controller seeking such acknowledgement.

2. In his application the controller must proceed as follows.

a) Clearly identify the data processing operation for which the exception is sought.

b) Explicitly describe the grounds that would justify acknowledgement.

c) Provide a detailed explanation of the measures proposed by the controller to guarantee citizens' rights.

3. The application must be submitted together with whatsoever documents or evidence are necessary to substantiate the existence of historical, scientific or statistical values justifying the Agency's acknowledgement.

Article 158. Duration of proceedings and effects of lack of an explicit resolution.

1. A resolution must be delivered and notice thereof served within three months counting from the date of receipt of the controller's request by the Spanish Data Protection Agency.

2. If no explicit resolution is delivered or notice served within the above term, the controller shall regard his request to be granted.

Sole additional provision. Software products.

The technical description of software products intended for automatic personal data processing must include the low, medium or high security level that can be reached therewith, pursuant to the provisions of Title VIII of these regulations.

Sole final provision. Subsidiary application.

For all issues not covered in Title IX, Chapter III, the Spanish Data Protection Agency's power to impose penalties shall be governed by the provisions of the Regulations for the Procedure for the Exercise of the Power to Impose Penalties, adopted under Royal Decree 1398/1993 of 4 August.