ROYAL DECREE 1720/2007, OF 21 DECEMBER, WHICH APPROVES THE REGULATION IMPLEMENTING ORGANIC LAW 15/1999, OF 13 DECEMBER, ON THE PROTECTION OF PERSONAL DATA

Ministry of Justice (Official Spanish Gazette No 17 of 19 January 2008)

Royal Decree 1720/2007, of 21 December, which approves the Regulation implementing Organic Law 15/1999, of 13 December, on the Protection of Personal Data.

The current Organic Law 15/1999, of 13 December, on the Protection of Personal Data adapted our legal system to the provisions of Directive 95/46/EC, of the European Parliament and of the Council, 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, at the same time repealing the previous Organic Law 5/1992, of 29 October, regulating the automatic processing of personal data.

The new Law, intended to have a wide scope indeed, provides in Article 1 that "[This Organic Law] is intended to guarantee and protect, with regard to the processing of personal data, the public liberties and fundamental rights of individuals, and in particular their honour and personal privacy". It includes, therefore, automated and non-automated processing of personal data.

In order to guarantee the necessary legal certainty in an area as sensitive for fundamental rights as that of data protection, the legislative declared the existing regulatory provisions should remain in force and, specifically, Royal Decrees 428/1993, of 26 March, which approve the Statutes of the Spanish Data Protection Agency, 1332/1994, of 20 June, which implements certain aspects of Organic Law 5/1992, of 29 October, regulating the automated processing of personal data and 994/1999, of 11 June, which approves the Regulation on Mandatory Security Measures for the Computer Files which contain Personal Data, as well as enabling the Government to approve or amend the necessary regulatory provisions for the application and implementation of Organic Law 15/1999.

Moreover, Act 34/2002, of 11 July, on Information Society Services and Electronic Commerce and the State Telecommunications Act 32/2003, of 3 November, gave the Spanish Data Protection Agency the power to impose sanctions. These require enabling regulations, with the unusual characteristic that both Acts are passed for the protection of the rights of legal entities as well as natural persons.

II

This Regulation and the Organic Law share the purpose of dealing with the risks to rights of identity arising from collecting and processing personal data. For this reason it must be emphasised that this Regulation is not intended to repeat the contents of the superior law but to implement not only the provisions of the Organic Law pursuant to the principles emanating

from the Directive, but also those that have shown over the years this Act has been in force, that they require greater legal implementation.

Therefore, this Regulation is approved based on the need to provide greater coherence to the regulation of everything relating to the transposition of the Directive and to implement the new aspects of Organic Law 15/1999, together with those that experience tells us require a degree of precision to provide legal certainty to the system.

III

The Regulation covers the area previously protected by Royal Decrees 1332/1994, of 20 June, and 994/1999, of 11 June, bearing in mind the need to set criteria applicable to non-automated files and processing of personal data. Moreover, the conferment of powers to the Spanish Data Protection Agency by Act 34/2002, of 11 July, on Information Society Services and Electronic Commerce and the State Telecommunications Act 32/2003, of 3 November, also obliges the implementation of the procedures through which the Agency can exercise its legal authority to impose sanctions.

The regulation is structured in nine Titles that implement the essential aspects of the subject.

Title I contemplates the purpose and scope of application of the Regulation. Throughout the validity of Organic Law 15/1999, the convenience of developing Article 2(2) has been noticed, in order to clarify the meaning of 'filing system' and 'processing' relating to personal or household activities; a particularly important aspect as they are excluded from the regulation on protection of personal data.

On the other hand, this Regulation does not contain provisions for the processing of personal data to which Article 2(3) of the Organic Law refers, as this is subject to specific regulations and the special provisions, as appropriate, of Organic Law 15/1999. As a result, the specific legal system for this processing and for these files is maintained.

This Title also provides a set of definitions that help the correct understanding of the Regulation, which is particularly necessary in such a technical field as the protection of personal data. It also lays out the criteria to follow for the calculation of time limits in order to standardise this matter, thus avoiding distinctions that result in differences in processing public and private files.

Title II refers to the principles of data protection. The regulation attaches particular importance to the manner of obtaining consent, dealing with very specific aspects such as the case of electronic communications services and, in particular, the obtaining of data relating to minors. Similarly, it offers what can only be defined as a Data Processor Statute, which no doubt shall help to clarify everything relating to this concept. The provisions in this area are completed by those provided in Title VIII regarding security, giving a coherent framework within which the data processor may act.

Title III deals with the essential question of the rights of persons in this area. These rights of access, rectification, erasure and objection to processing, as the Constitutional Court has affirmed in its Ruling number 292/2000, constitute the set of powers which stem from the fundamental right to the protection of data and "serve as the main function of this fundamental right: to guarantee to a person the power to control his personal data, which is only possible and effective by imposing on third parties the aforesaid compliance requirements".

Next, Titles IV and VII clarify important aspects for ordinary traffic, such as the application of specific criteria on certain types of privately-owned files, which require them due to their importance - those relating to financial solvency and creditworthiness and those used in advertising and commercial research; the set of material and formal obligations which should lead data controllers to create and register files; the criteria and procedures for carrying out international f data transfers; and, finally, the regulation of an instrument, a code of conduct, required to play an increasingly more important role as a dynamic force behind the fundamental right to data protection.

Title VIII regulates an essential aspect for the safeguarding of the fundamental right to data protection, security, which has repercussions on many organisational, management and even investment aspects, in all enterprises that process personal data. The importance of the duty of security obliged great rigour as different yet very important elements have converged on this matter. On the one hand, the experience arising from the application of Royal Decree 994/1999 made known the difficulties faced by data controllers and allowed the strong and weak points of the regulations to be identified. On the other hand, adaptation of various aspects of the regulations was called for. In this sense, the Regulation tries to be particularly rigorous in the assignment of the levels of security, in setting the measures that must be adopted in each case and in their review when necessary. It is also more precise in regulating the content and obligations associated with the maintenance of the security document. It also intends to regulate the matter in such a way that it considers the many forms of material and personal organisation of security in common practice. Finally, it regulates a set of measures aimed at structured, non-automated files and processing providing data controllers with a clear framework in which to act.

Finally, in Title IX, addressing the procedures handled by the Spanish Data Protection Agency, the decision has been made to specifically regulate those specialities that distinguish the different procedures handled by the Agency from the general laws provided for procedures in Act 30/1992, of 26 November, regulating Public Administrations and the Common Administrative Procedure, the application of which is declared subsidiary to this Regulation.

By virtue thereof, upon the proposal of the Minister of Justice, with the prior approval of the Minister for the Public Administrations, in agreement with the Council of State and following deliberation by the Council of Ministers at its meeting held on 21 December 2007;

I DO HEREBY DECREE:

SOLE ARTICLE. APPROVAL OF THE REGULATION

The Regulation implementing Organic Law 15/1999, of 13 December, on the protection of personal data is hereby approved, its text being included below.

FIRST TRANSITIONAL PROVISION. ADAPTATION OF THE CODES OF CONDUCT RECORDED WITH THE GENERAL DATA PROTECTION REGISTRY.

Within one year from the entry into force of this Royal Decree, the Spanish Data Protection Agency must be notified of the necessary amendments to the codes of conduct entered on the General Data Protection Registry to adapt their content to the provisions of Title VII of the same.

SECOND TRANSITIONAL PROVISION. IMPLEMENTATION TIME LIMITS FOR SECURITY MEASURES.

The security measures provided herein must be implemented pursuant to the following rules:

1. Regarding automated files in existence on the date of entry into force of this Royal Decree:
    a. The medium-level security measures must be implemented within one year of its entry into force, required for the following files:
        1. Those controlled by Management Agencies and Common Services of the Social Security and which relate to the exercise of their powers;
        2. Those controlled by Mutual Funds for accidents at work and occupational illness associated with the Social Security;
        3. Those containing a set of personal data providing a definition of the characteristics of identity of citizens and which allow certain aspects of their identity or behaviour to be assessed, regarding the measures of this level that were not applicable pursuant to the provisions of Article 4.4 of the Regulation on Mandatory Security Measures for the Computer Files which contain Personal Data, approved by Royal Decree 994/1999, of 11 June.
    b. The medium-level security measures must be implemented within one year of its entry into force and the high-level measures within eighteen months of that date, regarding the following files:
        1. Those containing data arising from gender-based violence;

2. Those controlled by operators providing electronic communications services to the public or who use public electronic communication networks relating to traffic and location data.

c. In all other cases, when this Regulation requires the implementation of an additional measure, not provided for in the Regulation on Mandatory Security Measures for the Computer Files that contain Personal Data, approved by Royal Decree 994/1999, of 11 June, the measures must be implemented within one year from the entry into force of this Royal Decree.

2. Regarding non-automated files in existence on the date of entry into force of this Royal Decree:

a. Basic-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.

3. Automated and non-automated files created after the date of entry into force of this Royal Decree must have implemented all the security measures regulated herein from the moment it is created.

THIRD TRANSITIONAL PROVISION. TRANSITIONAL REGIME OF REQUESTS TO EXERCISE THE RIGHTS OF INDIVIDUALS.

This Royal Decree shall not be applicable to requests to exercise the rights of access, objection, rectification and erasure made before its entry into force. These requests shall be subject to the previous legislation.

FOURTH TRANSITIONAL PROVISION. TRANSITIONAL REGIME OF PROCEDURES.

This Royal Decree shall not be applicable to procedures started before its entry into force. These procedures shall be subject to the previous legislation.

FIFTH TRANSITIONAL PROVISION. TRANSITIONAL REGIME OF PRELIMINARY PROCEEDINGS.

This Royal Decree shall not be applicable to preliminary proceedings started before its entry into force. These proceedings shall be subject to the previous legislation.

This Royal Decree shall be applied to preliminary proceedings started after its entry into force.

SOLE REPEALING PROVISION. REPEAL OF REGULATIONS.

Royal Decree 1332/1994, of 20 June, implementing certain aspects of Organic Law 5/1992, of 29 October, regulating the automatic processing of personal data; Royal Decree 994/1999, of 11 June, which approves the Regulation on Mandatory Security Measures for the Computer Files which contain Personal Data; and all regulations of similar or lower status which contradict or oppose those provided herein, are hereby repealed.

FIRST FINAL PROVISION. POWERS USED.

Title I, with the exception of Article 4(c), Titles II, II, VII and VIII, as well as Articles 52, 53.3, 53.4, 54, 55.1, 55.3, 56, 57, 58 and 63.3 of the Regulation are made pursuant to the provisions of Article 149.1.1. of the Spanish Constitution, which gives the State exclusive jurisdiction for the regulation of the basic conditions that guarantee the equality of all Spaniards in the exercise of constitutional rights and in the fulfilment of constitutional duties.

SECOND FINAL PROVISION. ENTRY INTO FORCE.

This Royal Decree shall enter into force three months after its full publication in the Official Spanish Gazette.

Given at Madrid, this 21 December 2007.

JUAN CARLOS R.

The Minister of Justice
MARIANO FERNÁNDEZ BERMEJO

REGULATION IMPLEMENTING ORGANIC LAW 15/1999, OF 13 DECEMBER, ON THE PROTECTION OF PERSONAL DATA

TITLE I
General provisions

ARTICLE 1. PURPOSE.

1. The purpose of this Regulation is the implementation of Organic Law 15/1999, of 13 December, on the protection of personal data.

2. Similarly, Chapter III of Title IX hereof implements the provisions relating to the exercise by the Spanish Data Protection Agency of the power to impose penalties, in application of the provisions of Organic Law 15/1999, of 13 December, in Title VII of Act 34/2002, of 11 July, on Information Society Services and Electronic Commerce and in Title VIII of the State Telecommunications Act 32/2003, of 3 November.

ARTICLE 2. OBJECTIVE SCOPE OF APPLICATION.

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

2. This Regulation shall not be applied to data processing regarding legal entities, nor to the files that only record data of individuals providing services in them, comprising only their name and surname(s), functions or jobs performed, as well as the postal or e-mail address and professional telephone and fax numbers.

3. Similarly, data relating to sole traders, when referring to them as traders, industrialists or ship owners, shall also be excluded from application of the system of protection of personal data.

4. This Regulation shall not be applied to data regarding the deceased. The aforesaid notwithstanding, relatives or others similarly associated with the deceased may contact the data controllers of files or processing containing the deceased's data in order to inform them of the death, providing sufficient documentary proof, and requesting, where appropriate, erasure of the data.

ARTICLE 3. TERRITORIAL SCOPE OF APPLICATION.

1. This Regulation shall govern any processing of personal data:

a) When the processing is carried out as part of the activities of an establishment pertaining to the data controller, whenever the establishment is in Spanish territory.

When the provision in the previous subsection is not applicable, but the data processor is located in Spain, the rules contained in Title VIII hereof shall be applicable to him.

b) When the data controller is not established on Spanish territory but is subject to Spanish Law pursuant to the norms of Public International Law.

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

In this case, the data controller must designate a representative established in Spanish territory.

2. For the purposes provided in the previous subsections, establishment shall be considered, irrespective of its legal structure, as any stable installation allowing the effective and real execution of an activity.

ARTICLE 4. EXCLUDED FILES OR PROCESSING.

The system of protection of personal data established herein shall not be applied to the following files and processing:

a) Those created or maintained by a natural person in the exercise of activities which are exclusively personal or domestic.

Those relating to personal or domestic activities shall only be considered as processing relating to activities arising within the framework of the private or family life of individuals.

b) Those subject to the legislation on the protection of classified materials.

c) Those established for the investigation of terrorism and serious forms of organised crime. The aforesaid notwithstanding, in such cases, the data controller shall previously inform the Spanish Data Protection Agency of their existence, general characteristics and purpose.

ARTICLE 5. DEFINITIONS.

1. The following definitions shall apply for the purposes of this Regulation:

a) Data subject: the natural person to whom the data undergoing processing pertain.

b) Erasure: procedure through which the data controller stops using data. Erasure shall imply data being blocked, comprising their identification and retention in order to prevent processing with the exception of being at the disposal of public administrations, judges and courts for the purpose of determining any liability arising from processing, and only for the duration of such liability. On the expiry of such term, the data shall be deleted.

c) Assignment or communication of data: processing that implies disclosing the data to a person other than the data subject.

d) Data subject's consent: any free, unequivocal, specific and informed indication of his wishes by which the data subject consents to the processing of personal data relating to him.

e) Dissociated data: that not allowing identification of the data subject.

f) Personal data: any alphanumeric, graphic, photographic, acoustic or any other type of information pertaining to identified or identifiable natural persons.

g) Health-related personal data: information regarding the past, present and future health, physical or mental, of an individual. In particular, data referring to the level of disability and genetic information of a person are considered to relate to health.

h) Recipient: the natural person or legal entity, public or private or administrative body to which data are disclosed.

Entities without legal personality acting as separate parties in the operation may also be recipients.

i) Data processor: the natural person or legal entity, public or private, or administrative body that, alone or jointly with others, processes personal data on behalf of the data controller, due to the existence of legal relations binding them and delimiting the scope of his action for the provision of a service.

Entities without legal personality acting as separate parties in the operation may also be data processors.

j) Exporter of personal data: the natural person or legal entity, public or private, or administrative body situated in Spanish territory that carries out, pursuant to the provisions herein, a transfer of personal data to a third country.

k) Filing system: any structured set of personal data which are accessible according to specific criteria, whatever the form or method of its creation, storage, organisation and access.

l) Privately-owned filing systems: files controlled by persons, companies or private law entities, , irrespective of who owns their capital or the origin of their economic resources, as well as files controlled by public law corporations, as long as such files are not strictly associated with the exercise of public law powers attributed to them by their specific legislation.

m) Publicly-owned filing systems: files controlled by constitutional bodies with constitutional importance of the State or autonomous institutions with similar functions, local public administrations, as well as associated or dependent entities or bodies and public law Corporations, as long as their purpose is the exercise of public law powers.

n) Non-automated filing system: any set of personal data organised in a non-automated and structured manner pursuant to specific criteria regarding natural persons, that allows access without disproportionate effort to personal data, whether it is centralised, local or distributed by function or geographically.

ñ) Importer of personal data: the natural person or legal entity, public or private, or administrative body receiving the data in the event of their international transfer to a third country, whether it is the data controller, data processor or third party.

o) Identifiable person: any person who may be identified, directly or indirectly, through any information regarding his physical, physiological, psychological, economic, cultural or social identity. A natural person shall not be deemed identifiable if such identification requires disproportionate periods of time or activities.

p) Dissociation procedure: any data processing allowing dissociated data to be obtained.

q) Data controller: a natural person or legal entity, public or private, or administrative body, that alone or jointly with others decides on the purpose, content and use of the processing, although he does not effectively do it.

Entities without legal personality acting as separate parties in the operation may also be data controllers.

r) Third parties: the natural person or legal entity, public or private, or administrative body other than the data subject, the data controller, the data processor and the persons authorised to process the data under the direct authority of the data controller or data processor.

Entities without legal personality acting as separate parties in the operation may also be third parties.

s) International transfer of data: data processing that implies their transmission outside the territory of the European Economic Area, whether as an assignment or data disclosure, or for the purpose of data processing on behalf of the data controller established in Spanish territory.

t) Processing of data: any operation or technical process, whether automated or not, that allows the collection, recording, storage, creation, amendment, consultation, use, rectification, erasure, blocking or deletion, as well as the disclosure of data arising from communications, consultations, interconnections and transfers.

2. In particular, the following definitions shall apply regarding the provisions of Title VIII hereof:

a) Authorised access: authorisations granted to a user to use the various resources. If appropriate, these shall include authorisations or functions of a user delegated by the data controller or the security officer.

b) Authentication: procedure for checking a user's identity.

c) Password: confidential information, frequently formed by a line of characters that may be used in the authentication of a user or access to a resource.

d) Control of access: mechanism that depending on previously authenticated identification allows access to data or resources.

e) Backup copy: copy of the data in an automated file in a format that allows for its recovery.

f) Document: any written, graphic, audible, image or any other kind of information that may be processed in an information system as a separate unit.

g) Temporary files: working files created by users or processes that are necessary for occasional processing or as an intermediate stage during processing.

h) Identification: procedure of recognition of a user's identity.

i) Incident: any event that affects or may affect a user's identity.

j) User profile: authorised access to a group of users.

k) Resource: any component of an information system.

l) Security officer: person or persons to whom the data controller has formally assigned the task of co-ordinating and controlling the applicable security measures.

m) Information system: set of files, processes, programs, media and, if appropriate, equipment used for processing personal data.

n) System of processing: manner in which an information system is organised or used. Depending on the system of processing, information systems may be automated, non-automated o partially automated.

ñ) Support: physical object that stores or contains data or documents, or an object capable of being processed in an information system and on which data can be recorded and recovered.

o) Transfer of documents: any transfer, communication, despatch, delivery or dissemination of information contained therein.

p) User: subject or process authorised to access data or resources. Processes allowing access to data or resources without the identification of a physical user shall be considered users.

ARTICLE 6. COMPUTATION OF TIME LIMITS.

Should this Regulation establish a period of time in days, only working days shall be calculated. When the period of time is in months, calendar days shall be used.

ARTICLE 7. SOURCES ACCESSIBLE TO THE PUBLIC.

1. For the purposes of Article 3(j) of Organic Law 15/1999, only the following shall be deemed sources accessible to the public:

a) The promotional census, regulated pursuant to the provisions of Organic Law 15/1999, of 13 December.

b) Guides to electronic communications services, under the terms provided by the relevant legislation.

c) Lists of persons pertaining to professional groups only containing the following data: name, title, profession, activity, academic degree, professional address and indication of his membership of the group. The professional address may include data on the complete postal address, telephone number, fax number and e-mail address. Regarding professional associations, data regarding membership of the association may include the membership number, date of joining and professional practice status.

d) Official journals and gazettes.

e) The Media.

2. In any case, for the aforesaid sources to be considered sources accessible to the public, it is essential that they may be consulted by any person, that they are not subject to restrictive legislation, or only require the payment of a consultation fee.

TITLE II
Principles of data protection

CHAPTER I
Quality of the data

ARTICLE 8. DATA QUALITY PRINCIPLES.

1. Personal data must be processed fairly and lawfully. The collection of data by fraudulent, unfair or illicit means is hereby prohibited.

2. Personal data may only be collected for specified, explicit and legitimate purposes of the data controller.

3. Personal data subjected to processing may not be used for purposes incompatible with those for which they were collected.

4. Personal data may only be processed if they are adequate, relevant and not excessive in relation to the specific, explicit and legitimate purposes for which they were obtained.

5. Personal data shall be accurate and updated in such a way as to give a true picture of the current situation of the data subject. If data are collected directly from the data subject, they shall be considered accurate.

If personal data subjected to processing prove to be inaccurate, either in whole or in part, or incomplete, they shall be erased and replaced ex- officio by the relevant rectified or complete data within ten days of being informed of the inaccuracy, unless the legislation applicable to the files establishes a specific procedure or deadline.

When data have been previously communicated, the data controller shall notify the recipient, within ten days, of the rectification or erasure, whenever the recipient is known.

Within ten days from receipt of the notification, the recipient of the data processing shall rectify and erase the relevant data.

Such updating of personal data shall not require any communication to the data subject, without prejudice to the rights granted to data subjects in Organic Law 15/1999, of 13 December.

The aforesaid provisions are considered without prejudice to the powers granted to data subjects in Title III hereof.

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

The aforesaid notwithstanding, they may be stored for the duration of any kind of liability arising from legal relations or obligations or the execution of a contract or the application of precontractual measures requested by the data subject.

On the expiry of such liability as stated above, data may only be stored following their dissociation, without prejudice to the obligation of blocking set out herein and in Organic Law 15/1999, of 13 December.

7. Personal data shall be processed in such a way as to allow the right of access to be exercised, until they are not due to be erased.

ARTICLE 9. PROCESSING FOR STATISTICAL, HISTORICAL OR SCIENTIFIC PURPOSES.

1. Processing of personal data for historical, statistical or scientific purposes shall not be considered incompatible, for the purposes set out in subsection 3 of the previous Article.

The purposes to which the previous paragraph refers shall be determined by the legislation applicable in each case and, in particular, by the provisions of Act 12/1989, of 9 May, regulating the Public Statistics Function, Act 16/1985, of 25 June, on the Spanish Historical Heritage and Act 13/1986, of 14 April, on the promotion and general coordination of scientific and technical research, and their respective provisions of implementation, as well as the legislation of the Autonomous Communities on these matters.

2. As an exception to the provisions of subsection 6 of the previous Article, the Spanish Data Protection Agency or, if appropriate, the supervisory authorities of the Autonomous Communities may, following a request by the data controller and pursuant to procedures established in section two of Chapter VII of Title IX hereof, decide to keep an entire set of specific data, bearing in mind their historical, statistical or scientific value pursuant to the rules to which the previous subsection refers.

ARTICLE 10. CASES WHICH LEGITIMISE THE PROCESSING OR ASSIGNMENT OF DATA.

1. Personal data may only undergo processing or assignment if the data subject has previously given his consent.

2. The aforesaid notwithstanding, processing or assignment of personal data shall be possible without the data subject's consent when:

a) It is authorised by a regulation having the force of Law or under Community Law and, in particular, when one of the following situations applies:

The purpose of the processing or assignment is to satisfy a legitimate interest of the data controller or recipient guaranteed by these rules, as long as the interest or fundamental rights and liberties of the data subjects as provided in Article 1 of Organic Law 15/1999, of 13 December, do not prevail.

The processing or assignment of data is necessary in order that the data controller fulfils a duty imposed upon him by one of the said laws.

b) The data object of processing or assignment are in sources accessible to the public and the data controller, or the third party to whom data has been communicated, has a legitimate interest in their processing or knowledge, as long as the fundamental rights and liberties of the data subject are not breached.

The aforesaid notwithstanding, the public administrations may only communicate the data collected from sources accessible to the public to the data controllers of privately-owned files under the aegis of this subsection, when they are so authorised by a regulation having the force of Law.

3. Consent of the data subject shall not be required for the processing of personal data when:

a) They are collected for the functions proper to public administrations within the scope of the powers given to them by a regulation having the force of Law or Community Law.

b) They are collected by the data controller for the purpose of executing a contract or preliminary contract or due to the existence of a business, employment or administrative relationship to which the data subject is party and are necessary for its maintenance or fulfilment.

c) The purpose of the data processing is to protect an essential interest of the data subject under the terms of Article 7(6) of Organic Law 15/1999, of 13 December.

4. Consent of the data subject shall not be required for the disclosure of his personal data when:

a) The assigment is due to the free and legitimate acceptance of a legal relationship that necessarily entails the communication of the data for its life, fulfilment and monitoring. In that case, disclosure shall be legitimate to the extent of the purpose justifying it.

b) The asigment to be effected is destined for the Ombudsman, the Office of the Public Prosecutor, judges, courts or the Spanish Court of Audit or to the institutions of the Autonomous Communities with similar functions to that of the Ombudsman or Spanish Court of Audit and it is done within the scope of the functions expressly assigned to them by law.

c) The assignment between public administrations when one of the following situations applies:

Processing of the data is for historical, statistical or scientific purposes.

The personal data has been collected or drawn up by one public administration to be sent to another.

The communication is done in order to exercise identical powers or powers relating to the same matters.

5. Specially protected data may be processed and disclosed under the terms provided in Articles 7 and 8 of Organic Law 15/199, of 13 December.

In particular, consent of the data subject shall not be required for the communication of health-related personal data, including via electronic means, between bodies, centres and services of the Spanish National Health Service when it is for the purpose of medical care of the persons, pursuant to the provisions of Chapter V of Act 16/2003, of 28 May, on the cohesion and quality of the Spanish National Health Service.

ARTICLE 11. VERIFICATION OF DATA IN REQUESTS MADE TO THE PUBLIC ADMINISTRATIONS.

When requests are drawn up by electronic means in which the data subject declares personal data held by the public administrations, the body receiving the request may carry out in the exercise of its powers the necessary verifications to ensure the authenticity of the data.

CHAPTER II
Consent for the processing of data and information to be given to the data subject

Section One. Obtaining the data subject's consent

ARTICLE 12. GENERAL PRINCIPLES.

1. The data controller shall obtain the data subject's consent for the processing of his personal data except in those situations where it does not have to be obtained pursuant to that provided at law.

The request for consent shall refer to specific processing or series of processes, stating the purpose for which they are collected, as well as the other conditions applying to the processing or series of processes.

2. When consent of the data subject is requested for the assignment of his data, he shall be informed in such a way as to understand unequivocally the purpose for which the relevant data shall be used and the type of activity performed by the recipient. Otherwise, consent shall be null and void.

3. The data controller shall be responsible for proving the existence of the data subject's consent by any means of legally admissible evidence.

ARTICLE 13. CONSENT FOR THE PROCESSING OF DATA OF MINORS.

1. Data pertaining to data subjects over fourteen years of age may be processed with their consent, except in those cases where the law requires the assistance of parents or guardians in the provision of such data. The consent of parents or guardians shall be required for children under fourteen years old.

2. Under no circumstances may data be collected from the minor regarding information about any other member of the family unit, or about its characteristics, such as data relating to the professional activity of the parents, financial information, sociological or any other such data, without the consent of the persons to whom such data refer. The aforesaid notwithstanding, data regarding the identity and address of the father, mother or guardian may be collected for the sole purpose of obtaining the authorisation set out in the previous subsection.

3. When processing refers to the data of minors, the information aimed at them shall be expressed in easily understandable language, with express indication of the provisions of this Article.

4. The data controller is responsible for setting up the procedures that guarantee that the age of the minor and authenticity of the consent given by the parents, guardians or legal representatives have been effectively checked.

ARTICLE 14. METHOD OF OBTAINING CONSENT.

1. The data controller may request the data subject's consent through the procedure set out in this article, unless he is required by Law to obtain the express consent for the processing of the data.

2. The data controller may contact the data subject, informing him of the terms provided in Articles 5 of Organic Law 15/1999, of 13 December and 12.2 herein and shall grant him thirty days to indicate his objection to the processing, advising him that should no objection be received it shall be considered that he consents to the processing of his personal data.

In particular, when this refers to data controllers providing the data subject with a service that generates periodic or repeat information, or periodic billing, the communication may be carried out jointly with this information or with the billing for the service provided, as long as it is done in a visible manner.

3. In any case, the data controller shall necessarily have to be informed whether the communication has been returned for any reason, in which case he may not proceed with the processing of the data regarding that data subject.

4. The data subject shall be provided with a simple and free means of stating his objection to the data processing. In particular, the requirements of this Regulation shall be considered met by those procedures whereby the objection can be made, among others, by sending a prepaid

letter addressed to the data controller or by calling a free telephone number or public helpline service the data controller has established.

5. When consent of the data subject is requested through a procedure established in this Article, the data controller is not allowed to repeat the request for the same processing and for the same purposes within one year from the data of the previous request.

ARTICLE 15. REQUEST FOR CONSENT WITHIN A CONTRACTUAL RELATIONSHIP FOR PURPOSES NOT DIRECTLY RELATED

If the data controller requests the data subject's consent during the process of drawing up a contract for purposes that have no direct link to the maintenance, course or monitoring of the contractual relationship, he must allow the data subject to expressly indicate his objection to the processing or data disclosure.

In particular, compliance with this duty shall be deemed made when the data subject may tick a clearly visible box that is not already ticked in the document he is given for execution of the contract, or an equivalent procedure is established by which he may indicate the objection to the processing.

ARTICLE 16. PROCESSING OF INVOICING AND TRAFFIC DATA IN ELECTRONIC COMMUNICATION SERVICES.

The request for consent for the processing or disclosure of data of traffic, invoicing and location by the bound subjects, or in the event of its revocation, according to the legislation regulating telecommunications shall be subject to the provisions of the relevant legislation and, where it is not contrary thereto, to the provisions established herein.

ARTICLE 17. REVOCATION OF CONSENT.

1. The data subject may revoke his consent through free and simple means that do not imply any payment whatsoever to the data controller. In particular, the requirements of this Regulation shall be deemed met by those procedures whereby the objection can be made, among others, by sending a prepaid letter addressed to the data controller or by calling a free telephone number or public helpline service the data controller has established.

The following shall not be considered pursuant to the provisions of Organic Law 15/1999, of 13 December: establishment by the data controller of the requirement to send registered letters or similar despatches, use telecommunications services that involve an additional charge to the data subject or any other means involving an additional cost to the data subject as the means whereby he may object to the processing.

2. The data controller shall cease the processing of data within ten days from receipt of the revocation of consent, without prejudice to his obligation to block the data pursuant to the provisions of Article 16.3 of Organic Law 15/1999, of 13 December.

3. Should the data subject request confirmation of the cessation of the processing of his data, the data controller shall expressly answer the request.

4. If the data has been previously assigned, the data controller, once consent has been revoked, shall communicate it to the recipients within the time limit provided in subsection 2, so that they may cease the processing of the data should they still hold them, pursuant to Article 16.4 of Organic Law 15/1999, of 13 December.

Section Two. Information to be given to the data subject

ARTICLE 18. ACCREDITATION OF COMPLIANCE WITH THE DUTY OF INFORMATION.

1. The duty of information to which Article 5 of Organic Law 15/1999, of 13 December, refers shall be carried out using means that can prove its fulfilment and shall be kept throughout the duration of the processing of the data subject's data.

2. The data controller shall keep the support on which compliance with the duty to inform is recorded. The data controller may use computer or telematic media to store such supports. In particular, paper documents may be scanned, as long as there is a guarantee that no alteration to the original documents has been made during the scanning process.

ARTICLE 19. SPECIAL CASES.

Should the data controller change as a result of an operation of merger, demerger, global assignment of assets and liabilities, contribution or transfer of business or branch of business activity, or any corporate restructuring operation of a similar nature contemplated by company law, a disclosure of data shall not be deemed to have occurred, without prejudice to compliance by the data controller of the provisions of Article 5 of Organic Law 15/1999, of 13 December.

CHAPTER III
The data processor

ARTICLE 20. RELATIONS BETWEEN THE DATA CONTROLLER AND DATA PROCESSOR.

1. Access to data by a data processor that is necessary for the provision of a service to the data controller shall not be considered comnunication of data, as long as there is compliance with the provisions of Organic Law 15/1999, of 13 December and those contained in this Chapter.

The service provided by the data processor may or may not be remunerated and may be temporary or permanent.

The aforesaid notwithstanding, data communication shall be considered to exist when the purpose of the access is to establish a new relationship between whoever accesses the data and the data subject.

2. When the data controller engages the provision of a service entailing processing of personal data subject to the provisions of this Chapter, he shall ensure that the data processor complies with all the guarantees for compliance with that provided herein.

3. Should the data processor use the data for another purpose, disclose or use them in breach of the stipulations of the contract to which Article 12(2) of Organic Law 15/1999, of 13 December, refers, he shall also be considered the data controller, answering for the breaches he has personally caused.

The aforesaid notwithstanding, the data processor shall not be liable when, following the express indication of the data controller, he discloses the data to a third party designated by the data controller, to whom he has commissioned the provision of a service pursuant to the provisions of this Chapter.

ARTICLE 21. POSSIBILITY OF SUBCONTRACTING SERVICES.

1. The data processor may not subcontract to a third party any processing commissioned to him by the data controller, unless he has received authorisation to do so. In that case, the contracting shall always be done in the name and on behalf of the data controller.

2. Notwithstanding the previous subsection, subcontracting shall be possible without the need for authorisation whenever the following requirements are met:

a) The contract specifies what services may be subject to subcontracting and, where possible, the company to which they shall be subcontracted.

   When the subcontracted company is not identified in the contract, the data processor shall inform the data controller of its identifying data before proceeding with the subcontracting.

b) The processing of the personal data by the subcontractor follows the instructions of the data controller.

c) The data processor and the subcontracted company formalise the contract, under the terms provided in the previous Article.

   In that case, the subcontractor shall be deemed the data processor, the provisions of Article 20.3 hereof being applicable to him.

3. If during the provision of the service it is necessary to subcontract a part of it and these circumstances have no provision in the contract, the points set out in the previous subsection shall be submitted to the data controller.

ARTICLE 22. STORAGE OF DATA BY THE DATA PROCESSOR.

1. Once the contractual provision has been fulfilled, the personal data shall be destroyed or returned to the data controller or his designated data processor, together with any medium or document recording any personal data subject to processing.

The data shall not be destroyed when there is a legal provision requiring their storage, in which case they shall be returned and the data controller shall guarantee their storage.

2. The data processor shall store the data, duly blocked, whilst any liability may arise from the relations with the data controller.

TITLE III
Rights of access, rectification, erasure and objection

CHAPTER I
General provisions

ARTICLE 23. PERSONAL NATURE.

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

2. Such rights shall be exercised:

a) By the data subject, proving his identity in the manner provided in the following Article.

When the data subject is incapacitated or is a minor so he cannot exercise these rights personally, they may be exercised by his legal representative, who shall necessarily accredit his status as such.

b) The rights may also be exercised through a voluntary representative, expressly designated for the exercise of the right. In that case, the identity of the represented party shall be clearly accredited, through the provision of a copy of his Spanish National Identity Document or equivalent document, and the representation he confers.

c) When the data controller is a body of the public administrations or the Justice Administration, representation may be accredited by any means valid at law that is reliably recorded, or through a declaration in person of the data subject.

3. The rights shall be refused when the request is made by a person other than the data subject and evidence is not provided that he is representing the data subject.

ARTICLE 24. GENERAL CONDITIONS FOR EXERCISING THE RIGHTS OF ACCESS, RECTIFICATION, ERASURE AND OBJECTION.

1. The rights of access, rectification, erasure and objection are independent rights, meaning that none of them has to be exercised as a prior requirement for the exercise of another.

2. The data subject shall be granted a free and simple means of exercising the rights of access, rectification, erasure and objection.

3. The exercise by the data subject of his rights of access, rectification, erasure and objection shall be free of charge and under no circumstances shall it involve an additional payment to the data controller before whom they are exercised.

The following shall not be considered pursuant to the provisions of Organic Law 15/1999, of 13 December and those herein: establishment by the data controller of the requirement to send registered letters or similar, the use of telecommunications services that involve an additional charge to the data subject or any other means involving an excessive cost to the data subject as the means whereby he may exercise his rights.

4. When the data controller has any kind of customer or complaint services, related with the service provided or the products offered, he may grant data subjects the possibility of exercising their rights of access, rectification, erasure and objection through these services. In that case, the identity of the data subject shall be deemed accredited by the means established for the identification of the clients of the data controller in the provision of his services or purchase of his products.

5. The data controller shall deal with requests for access, rectification, erasure or objection exercised by data subjects even when they have not used the procedure specifically established by the data controller for this purpose, whenever they have used means that accredit the despatch and receipt of the request, and the request contains the elements to which paragraph 1 of the following Article refers.

ARTICLE 25. PROCEDURE.

1. With the exception of the situation to which paragraph 4 of the previous Article refers, the exercise of the rights shall be carried out through communication addressed to the data controller, which shall contain:

a) Name and surname(s) of the data subject; photocopy of his national identity document, or his passport or other valid identifying document and, if necessary, of the person representing him, or equivalent electronic instruments; as well as the document or electronic instrument accrediting such representation. The use of the identifying electronic signature of the data subject shall excuse the need to present the photocopies of the national identity document or equivalent document.

The previous paragraph shall be understood without prejudice to the specific legislation applying to identity data verification by the public administrations in administrative procedures.

b) Petition in which the request is specified.

c) Address for notification purposes, the date and signature of the person making the request.

d) Documents accrediting the petition made, if appropriate.

2. The data controller shall answer any request addressed to him, whether or not data subject's personal data appears in his files.

3. Should the request not comply with the requirements specified in subsection one, the data controller shall request their remedy.

4. The answer shall be pursuant to the requirements provided for each case in this Title.

5. The data controller shall be responsible for proving the fulfilment of the duty to respond to which subsection 2 refers, having to keep the proof of fulfilment of the said duty.

6. The data controller shall adopt the relevant measures to guarantee that his staff with access to personal data can provide information of the procedure a data subject must follow in order to exercise his rights.

7. The exercise of the rights of access, rectification, erasure and objection may be modulated for reasons of public safety in the cases and within the scope provided at law.

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

ARTICLE 26. EXERCISING RIGHTS BEFORE A DATA PROCESSOR.

When a data subject exercises his rights before a data processor and request the exercise of his right before him, the data processor shall notify the request to the data controller, so that it may be answered, unless the relationship existing with the data controller specifically provides that the data processor shall deal with, on behalf of the data controller, requests by data subjects to exercise their rights of access, rectification, erasure or objection.

CHAPTER II
Right of access

ARTICLE 27. RIGHT OF ACCESS.

1. The right of access is the right of the data subject to obtain information about whether his own personal data is subject to processing, the purpose of the processing that, if appropriate,

is being done, as well as the information available on the origin of such data and the communications made or planned for them.

2. By virtue of the right of access the data subject may obtain from the data controller information regarding specific data, data included in a certain file, or the entire set of his data subjected to processing.

The aforesaid notwithstanding, when reasons of particular complexity justify it, the data controller may ask the data subject to specify the files for which he wishes to exercise the right of access, for which purpose he shall provide him a list of all the files.

3. The right of access is independent from that granted to data subjects by special laws and in particular by Act 30/1992, of 26 November, on the Legal System of the Public Administration and the Common Administrative Procedure.

ARTICLE 28. EXERCISING THE RIGHT OF ACCESS.

1. Upon exercising the right of access, the data subject may choose to receive the information through one or several of the following file consultation systems:

a) Screen display.

b) Letter, copy or photocopy sent by post, registered or not.

c) Facsimile.

d) E-mail or other electronic communication systems.

e) Any other system that is suitable to the configuration or material implementation of the filing system or to the nature of the processing, offered by the data controller.

2. The file consultation systems provided in the previous subsection may be restricted depending on the configuration or material implementation of the filing system or the nature of the processing, whenever that offered to the data subject is free and ensures written communication if so required.

3. Upon facilitating access the data controller shall comply with the provisions of Title VIII hereof.

Should the data controller offer a specific system for the effective exercise of the right of access and the data subject rejects it, the data controller shall not be liable for the possible risks to the security of the information that may arise from the choice.

Similarly, if the data controller offers a specific system for the effective exercise of the right of access and the data subject demands it be done through a procedure that involves a disproportionate cost, being similarly effective and guaranteeing the same security as the procedure offered by the data controller, the costs arising from such a decision shall be at the expense of the data subject.

ARTICLE 29. GRANTING ACCESS.

1. The data controller shall settle the request for access within one month from its receipt. On the expiry of this time limit, if the request for access has not been expressly answered, the data subject may file a claim provided in Article 18 of Organic Law 15/1999, of 13 December.

Should the data controller not hold data subject's personal data, he shall equally communicate this within the same period of time.

2. If the request is upheld and the data controller does not include in his communication the information to which Article 27.1 refers, access shall be made effective within the ten days following such communication.

3. The information provided, by whatever means, shall be legible and understandable, without using keys or codes that require the use of specific mechanical devices.

Such information shall comprise all the basic data of the data subject, those resulting from any computer process or preparation, as well as the information available on the origin of the data, their recipients and specification of the particular uses and purposes for which data has been stored.

ARTICLE 30. DENIAL OF ACCESS.

1. The data controller may deny access to the personal data when the right has already been exercised during the twelve months prior to the request, unless a legitimate interest is accredited for this purpose.

2. Access may also be denied if thus provided by law or a directly applicable community rule of law or when these prevent the data controller from disclosing to data subjects the processing of the data to which the access refers.

3. In any case, the data controller shall inform the data subject of his right to obtain the protection of the Spanish Data Protection Agency or, if appropriate, the supervisory authorities of the Autonomous Communities, pursuant to the provisions of Article 18 of Organic Law 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 the right of the data subject to have inaccurate or incomplete data amended.

2. The exercise of the right of erasure shall give rise to the deletion of data that is inadequate or excessive, without prejudice to the duty to blocking pursuant to this Regulation.

Should the data subject call for the exercise of the right of erasure to revoke previously given consent, the provisions of Organic Law 15/1999, of 13 December and those herein shall be applied.

ARTICLE 32. EXERCISING THE RIGHTS OF RECTIFICATION AND ERASURE.

1. The request for rectification shall indicate to which data it refers and the correction to be made and shall include the documentation justifying the request.

In the request for erasure, the data subject shall indicate to which data it refers, providing the documentation justifying the request, if appropriate.

2. The data controller shall settle the request for rectification or erasure within ten days from receipt of the request. On the expiry of this time limit if the request has not been expressly answered, the data subject may file a claim as provided in Article 18 of Organic Law 15/1999, of 13 December.

Should the data controller not hold data subject's personal data, he shall equally communicate this within the same period of time.

3. If the rectified or erased data has been previously assigned, the data controller shall communicate the rectification or erasure made to the recipient, within the same period of time, so that he may, also within ten days starting from receipt of such communication, proceed to similarly rectify or erase the data.

The rectification or erasure by the recipient shall not require any communication to the data subject, without prejudice to the exercise of the rights by the data subjects recognised in Organic Law 15/1999, of 13 December.

ARTICLE 33. DENIAL OF THE RIGHTS OF RECTIFICATION AND ERASURE.

1. Erasure shall be denied when the personal data must be stored for the periods of time provided in the applicable provisions or, if appropriate, in the contractual relations between the data controller and the data subject which justified the processing of the data.

2. The rights of rectification or erasure may also be denied if thus provided by law or a directly applicable community rule of law, or when these prevent the data controller from disclosing to data subjects the processing of the data to which the access refers.

3. In any case, the data controller shall inform the data subject of his right to obtain the protection of the Spanish Data Protection Agency or, if appropriate, the supervisory authorities of the Autonomous Communities, pursuant to the provisions of Article 18 of Organic Law 15/1999, of 13 December.

CHAPTER IV
Right to object

ARTICLE 34. RIGHT TO OBJECT.

The right to object is the right of the data subject that processing of his personal data be not carried out or be ceased in the following situations:

a) When his consent to the processing is not necessary, as a result of a legitimate and grounded reason, referring to his specific personal situation, which justifies it, unless otherwise provided by law.

b) When the purpose of the regarding files is to carry out advertising and commercial research activities, under the terms provided in Article 51 hereof, whatever the company responsible for its creation.

c) When the purpose of the processing is to make a decision regarding the data subject and is solely based on the automated processing of his personal data, under the terms provided in Article 36 hereof.

ARTICLE 35. EXERCISING THE RIGHT TO OBJECT.

1. The right to object shall be exercised through a request addressed to the data controller.

When the objection is based on letter a) of the previous Article, the request shall record the grounded and legitimate reasons, relating to a specific personal situation of the data subject, that justifies the exercise of this right.

2. The data controller shall settle the request for objection within ten days starting from receipt of the request. On the expiry of this time limit if the request has not been expressly answered, the data subject may file a claim as provided in Article 18 of Organic Law 15/1999, of 13 December.

Should the data controller not hold data subject's personal data, he shall equally communicate this within the same period of time.

3. The data controller shall exclude from the processing the data relating to the data subject who exercises his right to object, or shall deny the request of the data subject, with justification, within the period provided in subsection 2 of this Article.

ARTICLE 36. RIGHT TO OBJECT TO DECISIONS BASED SOLELY ON AUTOMATED DATA PROCESSING.

1. Data subjects have the right not to be subject to a decision which produces legal effects concerning them or significantly affects them, and wich is based solely on an automated processing of data intended to evaluate certain aspects relating to them, such as their performance at work, creditworthiness, reliability or conduct.

2. The aforesaid notwithstanding, data subjects may be subject to one of the decisions contemplated in subsection 1 when such a decision:

a) is made within the framework of the execution or implementation of a contract at the request of the data subject, whenever he is afforded the possibility of providing arguments that he may deem to be relevant, for the purpose of defending his right or interest. In any case, the data controller shall previously inform the data subject, clearly and precisely, that decisions shall be made with the characteristics highlighted in subsection 1 and shall erase the data in the event the contract is not entered into.

b) Is authorised by a regulation having the force of Law that establishes measures that guarantee the legitimate interest of the data subject.

TITLE IV
Provisions applicable to certain privately-owned files

CHAPTER I
Files of information regarding financial solvency and creditworthiness

´

Section One. General Provisions

ARTICLE 37. APPLICABLE SYSTEM.

1. The processing of personal data regarding financial solvency and creditworthiness, provided in Article 29.1 of Organic Law 15/1999, of 13 December, shall be subject to the general provisions contained in the said Organic Law and herein.

2. The exercise of the rights of access, rectification, erasure and objection regarding files to which the previous subsection refers, is governed by the provisions of Chapters I to IV of Title III hereof, with the following criteria:

a) When the petition to exercise the rights is addressed to the data controller, he shall be bound to satisfy such rights, in all cases.

b) If the request is addressed to the persons and entities to which the service is provided, they shall only disclose to the data subject those data relating to the data subject that they have received, and provide the identity of the data controller so that, if appropriate, the rights can be exercised before him.

3. Pursuant to Article 29.2 of Organic Law 15/1999, of 13 December, personal data relating to the fulfilment or non-fulfilment of pecuniary obligations provided by the creditor or the person acting on his behalf or interest, may also be processed.

These data shall be stored in files created for the sole purpose of providing credit-related information on the data subject and their processing shall be governed by that provided herein and, in particular, by the provisions contained in section two of this Chapter.

Section Two. Processing of data relating to the fulfilment or non-fulfilment of financial obligations provided by the creditor or the party acting on his behalf or interest.

ARTICLE 38. REQUIREMENTS FOR THE INCLUSION OF DATA.

Only personal data that are a determining factor for judging the financial solvency of the data subject may be included in these files, whenever the following requirements apply:

a) Prior existence of a verified, due, enforceable debt, that has not been paid and regarding which no legal, arbitration or administrative claim has been filed, or with regard to financial services, no claim has been filed under the terms provided in the Regulation of the Commissioners for the defence of the client of financial services, approved by Royal Decree 303/2004, of 20 February.

b) Six years have not passed from the date payment of the debt was due or from the expiry of the specific obligation or from a particular instalment deadline if regarding a periodic obligation.

c) Prior request for payment to whom fulfilment of the obligation corresponds.

2. Files of this nature may not include personal data for which there is preliminary evidence contradicting prima facie any of the previous requirements. This shall similarly lead to the precautionary erasure of the unfavourable personal data should it already have been included in the file.

3. The creditor or person acting on his behalf or interest shall be bound to store for provision to the data controller of the joint file and to the Spanish Data Protection Agency sufficient documentation that confirms the fulfilment of the requirements established herein and of the prior requirement to which the following Article refers.

ARTICLE 39. INFORMATION PRIOR TO INCLUSION.

The creditor shall inform the debtor, upon the formalisation of the contract and, in any case, upon making the request to which letter c) of subsection 1 of the previous Article refers, that should payment not be made under the terms provided for this purpose and the requirements provided in the aforesaid Article be fulfilled, the data relating to the non-payment shall be disclosed to files relating to the fulfilment or non-fulfilment of pecuniary obligations.

ARTICLE 40. NOTIFICATION OF INCLUSION.

1. The data controller of the joint file shall notify the data subjects for whom personal data has been registered, within thirty days from such registration, a reference of those data that have

been included, thus informing them of the possibility to exercise their rights of access, rectification, erasure and objection, under the terms established in Organic Law 15/1999, of 13 December.

2. Notification shall be made for each specific and particular debt whether or not it has the same or different creditors.

3. Notification shall be made through reliable, auditable and independent means of the notifying party, which permits the effective despatch to be accredited.

4. In any case, the data controller shall necessarily have to know whether the notification has been returned for any reason, in which case the personal data referring to that data subject may not be processed.

Returns whereby the recipient has refused to receive the despatch shall be deemed insufficient reason for data referring to a data subject not to be processed.

5. If the notification of inclusion is returned, the data controller of the joint file shall verify with the creditor entity that the address used for this notification corresponds to that contractually agreed with the client for the purpose of communications and shall not proceed with the processing of the data if the aforesaid entity does not confirm the accuracy of such data.

ARTICLE 41. CONSERVATION OF DATA.

1. Only data that provides a true picture of the debt situations at any specific time may be subject to processing.

The payment or fulfilment of the debt shall determine the immediate erasure of all data relating thereto.

2. In the remaining cases, the data shall be erased after six years have elapsed from the expiry of the specific obligation or from a particular instalment deadline if regarding a periodic obligation.

ARTICLE 42. ACCESS TO INFORMATION CONTAINED IN THE FILE.

1. The data contained in the joint file may only be consulted by third parties when they need to judge the financial solvency of the data subject. In particular, these circumstances shall be deemed to apply in the following situations:

a) The data subject maintains some kind of contractual relationship with the third party that has still not expired.

b) The data subject intends to execute a contract with the third party that involves the deferred payment of the price.

c) The data subject intends to contract the provision of a service with the third party involving periodic billing.

2. The third parties shall inform the persons where the situations contemplated in letters b) and c) apply, in writing, of their right to consult the file.

In the event of telephone contracting of products or services to which the previous paragraph refers, the information may be given in another form other than in writing, responsibility for proving the fulfilment of the duty of information residing with the third party.

ARTICLE 43. LIABILITY.

1. The creditor or the person acting on his behalf or interest shall ensure that all the requirements established in Articles 38 and 39 are met upon notifying the adverse data to the data controller of the joint file.

2. The creditor or the person acting on his behalf or interest shall be liable for the non-existence or inaccuracy of the data he has provided for inclusion in the file, under the terms provided in Organic Law 15/1999, of 13 December.

ARTICLE 44. EXERCISING THE RIGHTS OF ACCESS, RECTIFICATION, ERASURE AND OBJECTION.

1. The exercise of the rights of access, rectification, erasure and objection is subject to the provisions of Chapters I to IV of Title III hereof, without prejudice to the provisions contained in this Article.

2. When the data subject exercises his right of access in relation to the inclusion of his data in a file regulated by Article 29.2 of Organic Law 15/1999, of 13 December, the following rules shall be borne in mind:

1. If the request is addressed to the owner of the joint file, he shall communicate to the data subject all the data relating to him recorded in the file.
    a. In this case, the owner of the joint file shall, as well as fulfilling the provisions hereof, provide the evaluations and assessments regarding the data subject that have been disclosed in the last six months and the name and address of the recipients.
2. If the request is addressed to any other participant in the system, he shall communicate to the data subject all the data relating to him to which they have access, as well as the identity and address of the owner of the joint file so that the data subject may complete his right of access.

3. When the data subject exercises his rights of rectification or erasure in relation to the inclusion of his data in a file regulated by Article 29.2 of Organic Law 15/1999, of 13 December, the following rules shall be borne in mind:

1. If the request is addressed to the owner of the joint file, he shall take the relevant measures to transfer the request to the entity that has provided the data, so that it may answer the request. If the data controller for the joint file has not received an answer

from the entity within seven days, he shall proceed with the precautionary rectification or erasure of the data.

2. If the request is addressed to the provider of the data to the joint file he shall proceed with the rectification or erasure of the data in his files and shall notify the owner of the joint file within ten days, also answering the data subject under the terms provided in Article 33 hereof.

3. If the request is addressed to another participant in the system, who has not provided data to the joint file, this entity shall inform the data subject of this fact within ten days, also providing the identity and address of the owner of the joint file so that, if necessary, the data subject may exercise his rights before him.

CHAPTER II

Processing for advertising and commercial research activities

ARTICLE 45. DATA SUBJECT TO PROCESSING AND INFORMATION FOR THE DATA SUBJECT.

1. Those involved in collecting addresses, distributing documents, advertising, distance selling, commercial research and other analogous activities, as well as those carrying out these activities in order to market their own products or services or those of third parties, shall only use names and addresses or other personal data when they are found in one of the following cases:

a) They appear in any of the sources accessible to the public to which Article 3(j) of Organic Law 15/1999, of 13 December, and Article 7 of this Regulation refer, and the data subject has not stated his refusal or objection to the processing of his data for the activities described herein.

b) They have been provided by the data subjects directly or obtained with their consent for specific, explicit and legitimate purposes relating to the activity of advertising or commercial research, having informed the data subjects on the specific and precise sectors of activity about which they may receive information or advertising.

2. When the data come from sources accessible to the public and are used for the activity of advertising or commercial research, the data subject shall be informed in each communication sent to him of the origin of the data and the identity of the data controller as well as of the data subject's rights, indicating before whom they may be exercised.

For this purpose, the data subject shall be informed that his data has been obtained from sources accessible to the public and the entity from which they have been obtained.

ARTICLE 46. DATA PROCESSING IN ADVERTISING CAMPAIGNS.

1. So that an entity may directly carry out an advertising activity of its products or services among its clients the processing shall necessarily be covered by one of the situations contemplated in Article 6 of Organic Law 15/1999, of 13 December.

2. Should the entity contract or commission third parties to carry out a specific advertising campaign of its products or services, commissioning the processing of specific data, the following rules shall apply:

a) The data controller shall be the entity that commissions the campaign, if it sets the identifying parameters of the recipients of the campaign.

b) The data controller shall be the entity or entities contracted when they are solely responsible for setting the parameters.

c) Both entities shall be data controllers when they both intervene in setting the parameters.

3. In the situation contemplated above, the entity commissioning the advertising campaign shall adopt the necessary measures to ensure that the contracted entity has collected the data in compliance with the requirements provided in Organic Law 15/1999, of 13 December, and those herein.

4. For the purposes provided in this Article, identifying parameters of the recipients shall be deemed to be the variables used to identify the target or recipient audience of a commercial campaign or promotion of products or services allowing the individual recipients to be defined.

ARTICLE 47. PURGING OF PERSONAL DATA.

When two or more data controllers, themselves or through the commission of third parties, attempt to ascertain the clients of one or the other or several of them, without the consent of the data subjects, for promotion or marketing purposes of their products or services and through cross-processing of their files, the processing shall be deemed an assignment or communication of data.

ARTICLE 48. EXCLUSION FILES REGARDING THE TRANSMISSION OF COMMERCIAL COMMUNICATIONS.

Data controllers to whom the data subject has stated his objection to receiving advertising may keep the minimum data essential for identification purposes and adopt the necessary measures to avoid sending advertising.

ARTICLE 49. JOINT EXCLUSION FILES REGARDING THE TRANSMISSION OF COMMERCIAL COMMUNICATIONS.

1. The creation of joint files shall be possible, of a general or sectoral nature, where the object of processing is personal data necessary to avoid the despatch of commercial communications to data subjects who have stated their refusal or objection to receiving advertising.

For this purpose, the aforesaid files shall contain the minimum data essential to identify the data subject.

2. When the data subject indicates to a specific data controller his refusal or objection to his data being processed for advertising or commercial research purposes, he shall be informed of the existence of general or sectoral joint exclusion files, as well as of the identity and contact address of the data controller, and purpose of the processing,

The data subject may request his exclusion regarding a specific file or processing or his inclusion in general or sectoral joint exclusion files.

3. The data controller for the joint file shall process the data of the data subjects that have stated their refusal or objection to the processing of their data for advertising or commercial research purposes, complying with the remaining obligations established in Organic Law 15/1999, of 13 December, and those herein.

4. Those who intend to carry out processing relating to advertising or commercial research activities shall previously consult the joint files that may affect their action, in order to avoid processing the data of data subjects that have stated their refusal or objection to this processing.

ARTICLE 50. RIGHTS OF ACCESS, RECTIFICATION AND ERASURE.

1. The exercise of the rights of access, rectification and erasure in relation to processing associated with advertising and commercial research activities shall be subject to the provisions of Chapters I to IV of Title II hereof.

2. If the right is exercised before an entity that has commissioned a third party with carrying out a publicity campaign, it shall be bound, within ten days from receipt of the communication of the request to exercise the rights of the data subject, to communicate the request to the data controller so that he may grant the data subject his right within ten days from receipt of the communication, informing the data subject of this.

The provision set out in the previous paragraph shall be deemed to be without prejudice to the duty imposed on the entity mentioned above, in all cases, by paragraph two of Article 5.5 of Organic Law 15/1999, of 13 December.

ARTICLE 51. RIGHT TO OBJECT.

1. Data subjects shall have the right to object, upon request and without incurring charges, to the processing of their data, in which case they shall be removed from processing, erasing the information on them appearing therein, following a simple request.

The objection to which the previous paragraph refers shall be deemed without prejudice to the right of the data subject to revoke, when he deems appropriate, the consent he may have granted for the processing of the data.

2. For this purpose, the data subject shall be granted free and simple means to object to the processing. In particular, this requirement shall be deemed met when the rights may be exercised by calling a free telephone number or sending an e-mail.

3. When the data controller has any kind of customer or complaint services, related with the service provided or the products offered, he shall grant the data subject the possibility of exercising his right to object through these services.

The following shall not be considered pursuant to the provisions of Organic Law 15/1999, of 13 December: establishment by the data controller of the requirement to send registered letters or similar, the use of telecommunications services that involve an additional charge for the data subject or any other means involving an excessive cost to the data subject as the means whereby he may exercise his right to object.

In any case, the exercise by the data subject of his rights shall not involve an additional income to the data controller before whom they are exercised.

4. If the right to object is exercised before an entity that has commissioned a third party with carrying out a publicity campaign, it shall be bound, within ten days from receipt of the communication of the request to exercise the rights of the data subject, to communicate the request to the data controller so that he may grant the data subject his right within ten days from receipt of the communication, informing the data subject of this.

The provision set out in the previous paragraph shall be deemed to be without prejudice to the duty imposed on the entity mentioned above, in all cases, by paragraph two of Article 5.5 of Organic Law 15/1999, of 13 December.

TITLE V
Obligations prior to data processing

CHAPTER I
Creation, amendment or deletion of publicly-owned files

ARTICLE 52. PROVISION OR RESOLUTION FOR THE CREATION, AMENDMENT OR DELETION OF THE FILE.

1. The creation, amendment or deletion of publicly-owned files may only be done through a general provision or resolution published in the Official Spanish Gazette or corresponding official journal.

2. In any case, the provision or resolution shall be made and published prior to the creation, amendment or deletion of the file.

ARTICLE 53. FORM OF THE PROVISION OR RESOLUTION.

1. When the provision refers to General Administration of the State bodies or its associated or dependent agencies or bodies, it shall be in the form of a ministerial order or decision of the Head of the corresponding agency or body.

2. State Constitutional bodies shall be subject to the provisions of their regulations.

3. Files controlled by Autonomous Communities, local organisations and their associated or dependent agencies or bodies, public universities, as well as the bodies of the Autonomous Communities with analogous functions to the State Constitutional bodies, shall be subject to the provisions of their specific legislation.

4. The creation, amendment or deletion of files controlled by public law corporations and that relate to the exercise of their public law powers shall be done by resolution of its governing bodies, under the terms established in their respective Statutes, similarly being subject to publication in the Official Spanish Gazette or corresponding official journal.

ARTICLE 54. CONTENT OF THE PROVISION OR RESOLUTION.

1. The provision or resolution for the creation of the file shall contain the following points:

a) Identification of the filing system or processing, indicating its name, as well as a description of its purpose and planned usage.

b) The origin of the data, indicating the group of persons from which personal data shall be obtained or who are bound to supply such data, the data collection procedure and its legality.

c) The basic structure of the filing system through a detailed description of the identifying data, and if appropriate, of the specially protected data, as well as of the other

categories of personal data included therein and the processing system used in their organisation.

d) The planned communications of data, indicating if appropriate, the recipients or categories of recipients.

e) The planned international data transfers to third countries, indicating where appropriate, the target countries of the data.

f) The bodies responsible for the filing system.

g) The services or units before which the rights of access, rectification, erasure or objection may be exercised.

h) The basic-, medium- or high-level of security that is applicable, pursuant to the provisions of Title VIII hereof.

2. The provision or resolution of amendment of the filing system shall indicate the amendments made in any of the points to which the previous subsection refers.

3. The provisions or resolutions made for the deletion of filing systems shall establish the destination of the data or, if appropriate, the provisions for their destruction.

CHAPTER II

Notification and registration of publicly- or privately-owned files

ARTICLE 55. NOTIFICATION OF FILES.

1. All publicly-owned personal data files shall be notified to the Spanish Data Protection Agency by the competent body of the Administration controlling the filing system for their registration in the General Data Protection Register, within thirty days of the publication of the provision or resolution for creation in the corresponding official gazette.

2. Privately-owned personal data filing systems shall be notified to the Spanish Data Protection Agency by the individual or private entity that intends to create them, prior to their creation. Notification shall indicate the identification of the data controller, the identification of the filing system, its purposes and planned usage, the processing system used in their organisation, the group of persons about whom data are obtained, the procedure and origin of the data, the categories of data, the service or unit of access, indication of the basic-, medium- or high-level security measures that are applicable and, if appropriate, the identification of the data processor where the filing system is located and the recipients of assignments and international data transfers.

3. When the obligation to notify affect filing systems subject to the jurisdiction of the supervisory authority of an Autonomous Community that has created its own register of filing systems, the notification shall be done to the competent autonomous authority, which shall notify the registration to the General Data Protection Register.

The General Data Protection Register may request the aforesaid transfer from the supervisory authorities of the Autonomous Communities, otherwise proceeding with the ex- officio inclusion of the file in the Register.

4. Notification shall be done pursuant to the procedure established in section one of Chapter IV of Title IX herein.

ARTICLE 56. PROCESSING OF DATA ON DIFFERENT SUPPORTS.

1. Notification of a personal data filing system is independent of the processing used in its organisation and the support or supports used for processing the data.

2. When the personal data being processed is stored on different support media, automated and non-automated, or there is a copy on a non-automated support of an automated file, only one sole notification shall be required regarding the said filing system.

ARTICLE 57. FILING SYSTEMS WITH MORE THAN ONE DATA CONTROLLER.

When there is an intention to create a filing system with several persons or entities acting simultaneously as the data controller, each one shall notify the creation of the corresponding filing system, in order to proceed with its registration in the General Data Protection Register and, if appropriate, in the registers of filing systems created by the supervisory authorities of the Autonomous Communities.

ARTICLE 58. NOTIFICATION OF THE AMENDMENT OR DELETION OF FILING SYSTEMS.

1. The entry of the filing system shall be up-to-date at all times. Any amendment that affects the content of the filing system registration shall be previously notified to the Spanish Data Protection Agency or the competent autonomous supervisory authorities, in order to proceed with its registration in the corresponding register, pursuant to the provisions of Article 55.

2. When the data controller decides on deletion of the filing system, he shall notify this so that the entry in the corresponding filing system can be erased.

3. With regard to publicly-owned filing systems, amendments that affect any of the requirements provided in Article 55 or deletion of the filing system shall require the adoption of the corresponding provision or resolution prior to the notification, in the terms provided in Chapter I of this Title.

ARTICLE 59. MODELS AND SUPPORTS FOR THE NOTIFICATION.

1. The Spanish Data Protection Agency shall publish through the corresponding decision of the Director the electronic models or forms for notification of the creation, amendment or deletion of filing systems, which permit their presentation through telematic means or on paper, as well as the formats for the telematic communication of public filing systems by the supervisory

authorities of the Autonomous Communities, following consultation of the data protection authorities of the Autonomous Communities, pursuant to the provisions of Articles 55 and 58 hereof.

2. The electronic models or forms for notification may be obtained free of charge from the website of the Spanish Data Protection Agency.

3. The Director of the Spanish Data Protection Agency shall establish simplified notification procedures depending on the circumstances of the processing or type of filing system to which the notification refers.

ARTICLE 60. REGISTRATION OF THE FILING SYSTEMS.

1. The Director of the Spanish Data Protection Agency, at the proposal of the General Data Protection Register, shall issue a ruling accepting the registration, if appropriate, once the procedure provided in Chapter IV or Title IX has been followed.

2. The entry shall contain the code assigned by the Registrar, the identification of the data controller, the identification of the filing system or processing, description of its purposes and planned usage, the processing system used in the organisation, if appropriate, the group of persons about whom data are obtained, the procedure and origin of the data, the categories of data, the service or unit of access, and indication of the level of security measures that are applicable pursuant to the provisions of Article 81.

It shall also include, if appropriate, the identification of the data processor where the filing system is located and the recipients of disclosures and international transfers.

Publicly-owned filing systems shall also record the reference of the general provision by which they have been created and, if relevant, modified.

3. The registration of a filing system in the General Data Protection Register does not exempt the data controller from the fulfilment of the other obligations provided in Organic Law 15/1999, of 13 December, and other regulations.

ARTICLE 61. ERASURE OF THE REGISTRATION.

1. When the data controller communicates the deletion of the filing system, by virtue of the provisions of Article 58 hereof, the Director of the Spanish Data Protection Agency shall issue a ruling accepting erasure of the entry regarding the filing system, following the procedure established in section one of Chapter IV of Title IX.

2. The Director of the Spanish Data Protection Agency may, in exercise of his powers, resolve ex- officio to erase the entry regarding a filing system when circumstances justifying the impossible nature of its existence appear, following the procedure established in section two of Chapter IV of Title IX

ARTICLE 62. RECTIFICATION OF ERRORS.

The General Data Protection Register shall rectify at any time, ex- officio or at the request of data subjects, the material, factual or mathematical errors that may exist in the entries, pursuant to the provisions of Article 105 of Act 30/1992, of 26 November.

ARTICLE 63. EX- OFFICIO REGISTRATION OF PUBLICLY-OWNED FILES.

1. In exceptional situations for the purpose of guaranteeing the right to the protection of data of data subjects, and without prejudice to the obligation of notification, a specific filing system may be registered ex- officio in the General Data Protection Register.

2. For the provisions of the previous subsection to be applicable, the corresponding provision or resolution regulating the filing systems containing personal data shall have to be published in the relevant official gazette and comply with the requirements established in Organic Law 15/1999, of 13 December, and those herein.

3. The Director of the Spanish Data Protection Agency may, at the proposal of the General Data Protection Register, resolve to register a publicly-owned filing system in the Register, notifying this resolution to the body responsible for the filing system.

When registration refers to filing systems subject to the jurisdiction of the supervisory authority of an Autonomous Community that has created its own register of filing systems, the authority of the Autonomous Community shall be informed so that it may, if appropriate, proceed with the registration ex- officio.

ARTICLE 64. COLLABORATION WITH THE SUPERVISORY AUTHORITIES OF THE AUTONOMOUS COMMUNITIES.

The Director of the Spanish Data Protection Agency may enter into with the directors of the supervisory authorities of the Autonomous Communities the partnership agreements he deems relevant, in order to guarantee registration in the General Data Protection Register of the filing systems subject to the jurisdiction of such authorities.

TITLE VI
International transfers of data

CHAPTER I
General provisions

ARTICLE 65. FULFILMENT OF THE PROVISIONS OF ORGANIC LAW 15/1999, OF 13 DECEMBER.

An international transfer of data does not exclude under any circumstances whatsoever the application of the provisions contained in Organic Law 15/1999, of 13 December, and those herein.

ARTICLE 66. AUTHORISATION AND NOTIFICATION.

1. So that an international transfer of data may be considered pursuant to the provisions of Organic Law 15/1999, of 13 December, and those herein, it shall require the authorisation of the Director of the Spanish Data Protection Agency, which shall be granted whenever the exporter provides the guarantees to which Article 70 hereof refers.

The authorisation shall be granted pursuant to the procedure established in section one of Chapter V of Title IX hereof.

2. Authorisation shall not be required if:

a) The Country in which the importer is located offers an adequate level of protection pursuant to the provisions of Chapter II of this Title; or

b) The transfer is covered by one of the situations contemplated in subsections a) to j) of Article 34 of Organic Law 15/1999, of 13 December.

3. In any case, an international transfer of data shall be notified in order to proceed with its registration in the General Data Protection Register, pursuant to the procedure established in section one of Chapter IV or Title IX hereof.

CHAPTER II
Transfers to countries providing an adequate level of protection

ARTICLE 67. ADEQUATE LEVEL OF PROTECTION RESOLVED BY THE SPANISH DATA PROTECTION AGENCY.

1. Authorisation of the Director of the Spanish Data Protection Agency shall not be required for an international transfer of data when the rules applicable to the Country where the importer is located offer such adequate level of protection in the opinion of the Director of the Spanish Data Protection Agency.

The adequate nature of the level of protection offered by the country receiving the data shall be assessed bearing in mind all the circumstances of the transfer or category of the data transfer. In particular, the nature of the data, the purpose and duration of the processing or processes planned, the country of origin and the country of final destination, the general or sectoral rules of law valid in the third country in question, the content of the reports of the European Commission, as well as the professional rules and security measures in force in such countries shall all be taken into account.

The decisions of the Director of the Spanish Data Protection Agency resolving that a specific country provides an adequate level of protection of data shall be published in the Official Spanish Gazette.

2. The Director of the Spanish Data Protection Agency shall resolve the publication of the list of countries where the level of protection has been deemed comparable pursuant to the provisions of the previous subsection.

This list shall be published and updated by computerised or telematic means.

ARTICLE 68. ADEQUATE LEVEL OF PROTECTION DECLARED BY DECISION OF THE EUROPEAN COMMISSION.

Authorisation of the Director of the Spanish Data Protection Agency shall not be required for an international transfer of data where the importer is a person or entity, public or private, located in the territory of a Country where the European Commission has declared the existence of an adequate level of protection.

ARTICLE 69. TEMPORARY SUSPENSION OF TRANSFERS.

1. In the situations contemplated in the preceding Articles, the Director of the Spanish Data Protection Agency, pursuant to the powers vested upon him by Article 37.1 f) of Organic Law 15/1999, of 13 December, may decide, following a hearing with the exporter, the temporary suspension of the transfer of data to an importer located in a third country of which the existence of an adequate level of protection has been declared, when any of the following circumstances apply:

a) The Data Protection Authorities of the importing country, or any other competent body should the former not exist, decide that the importer has breached the data protection laws established in its domestic law;

b) There are rational indications that the laws or, if appropriate, the principles of data protection are being breached by the importer of the transfer and that the competent authorities in the country where the importer is located have not adopted or are not going to adopt in the future, the relevant measures to settle the case in question, having been warned of the situation by the Spanish Data Protection Agency. In this case the transfer may be suspended when to continue with it could generate an imminent risk of serious harm to data subjects.

2. The suspension shall be decided following the procedure established in section two of Chapter V of Title IX hereof.

In such cases, the decision of the Director of the Spanish Data Protection Agency shall be notified to the European Commission.

CHAPTER III

Transfers to countries that do not provide an adequate level of protection.

ARTICLE 70. TRANSFERS SUBJECT TO AUTHORISATION OF THE DIRECTOR OF THE SPANISH DATA PROTECTION AGENCY.

1. When the destination of the transfer is a country where the European Commission has not declared or the Director of the Spanish Data Protection Agency has not considered there to be an adequate level of protection, it shall be necessary to obtain the authorisation of the Director of the Spanish Data Protection Agency.

Authorisation of the transfer shall be processed pursuant to the procedure established in section one of Chapter V of Title IX hereof.

2. Authorisation may be granted if the data controller provides a written contract executed between the exporter and importer, in which the necessary guarantees regarding the protection of the private life of data subjects and of their fundamental rights and liberties are recorded, and the exercise of their respective rights is guaranteed.

For this purpose, the adequate guarantees shall be considered established by those contracts executed pursuant to the provisions of the Decisions of the European Commission 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 the Decisions of the Commission that comply with the provisions of Article 26.4 of Directive 95/46/EC.

3. In the situation contemplated in the previous subsection, the Director of the Spanish Data Protection Agency may deny or, pursuant to the powers conferred to him by Article 37.1 f) of Organic Law 15/1999, of 13 December, temporarily suspend the transfer, following a hearing with the exporter, when any of the following circumstances apply:

a) The situation of the protection of the fundamental rights and public liberties in the destination country or its legislation prevents the guarantee of the complete performance of the contract and the exercise by data subjects of the rights guaranteed by the contract; or

b) The recipient entity has previously breached the guarantees established in contractual clauses of this kind;

c) There are rational indications that the guarantees offered by the contract are not being or shall not be respected by the importer;

d) There are rational indications that the mechanisms of application of the contract are not or shall not be effective;

e) The transfer, or its continuation if it has started, could create a situation of risk of actual harm to data subjects.

The suspension shall be decided following the procedure established in section two of Chapter V of Title IX hereof.

The rulings of the Director of the Spanish Data Protection Agency that deny or suspend an international transfer of data due to the causes to which this subsection refers shall be notified to the European Commission when so required.

4. Authorisation may also be granted for international data transfers as provided in multi-national groups of companies when these have adopted internal regulations or rules that establish the necessary guarantees regarding the protection of the private life and the fundamental right of protection of data of data subjects, and fulfilment of the principles and exercise of the rights recognised in Organic Law 15/1999, of 13 December, and herein, are also guaranteed.

In this case, for the authorisation of the Director of the Spanish Data Protection Agency it shall be necessary that the rules or regulations are binding for the companies in the Group and are enforceable pursuant to the Spanish legal system.

In any case, the authorisation of the Director of the Spanish Data Protection Agency shall imply the enforceability of the provisions of the internal rules and regulations by the Agency, as well as by the data subjects whose data have undergone processing.

TITLE VII
Codes of conduct

ARTICLE 71. PURPOSE AND NATURE.

1. The purpose of the codes of conduct to which Article 32 of Organic Law 15/1999, of 13 December, refers is to adapt the provisions of the aforesaid Organic Law and those herein to the unique characteristics of the processing carried out by subscribers thereto.

For this purpose, they shall contain specific rules or standards that permit the harmonisation of the data processing done by subscribers, facilitate the exercise of the rights of the data subjects and favour compliance of the provisions of Organic Law 15/1999, of 13 December, and of those herein.

2. The codes of conduct shall have the status of codes of ethics or good professional practice and shall be binding on subscribers.

ARTICLE 72. INITIATIVE AND SCOPE OF APPLICATION.

1. The codes of conduct shall be voluntary.

2. The sectoral codes of conduct shall refer to all or part of the processing carried out by entities pertaining to the same sector, and shall be drawn up by representative organisations of the sector, at least within its territorial scope of application, and without prejudice to the powers of such entities to adjust the code of conduct to their particular characteristics.

3. The codes of conduct promoted by a company shall refer to all the processing it carries out.

4. The public administrations and Public Law corporations may adopt codes of conduct pursuant to the provisions of their applicable laws.

ARTICLE 73. CONTENT.

1. The codes of conduct shall be drawn up in clear and accessible terms.

2. The codes of conduct shall abide by current legislation and include, at least, with a sufficient degree of precision:

a) The clear and precise delimitation of its scope of application, the activities to which the code refers and the processing subject to it;

b) The specific provisions for the application of the principles of data protection;

c) The establishment of standards for the compliance by subscribers of obligations established in Organic Law 15/1999, of 13 December;

d) The establishment of procedures facilitating the exercise by data subjects of their rights of access, rectification, erasure and objection;

e) The determination of the assignments and international transfers of data that, if appropriate, are planned, indicating the guarantees that must be adopted;

f) Training actions on data protection aimed at those who process data, particularly with regard to their relationship with data subjects;

g) The mechanisms for supervision through which it guarantees compliance by subscribers of that established in the code of conduct, in the terms provided in Article 74 hereof.

3. In particular, the code shall contain:

a) Standard clauses for obtaining the consent of data subjects to the processing or disclosure of their data;

b) Standard clauses for informing data subjects of the processing, when the data is not obtained from them;

c) Models for the exercise by data subjects of their rights of access, rectification, erasure and objection;

d) Models of clauses for compliance with the applicable formal requirements for contracting a data processor, if appropriate.

ARTICLE 74. ADDITIONAL COMMITMENTS.

1. The codes of conduct may include any other additional commitment taken on by the subscribers for better compliance with the current legislation on data protection.

2. They may also contain any other commitment established by the promoting entities and, in particular, on:

a) The adoption of additional security measures to those required in Organic Law 15/1999, of 13 December, and those herein;

b) The identification of the categories of recipients or importers of data;

c) The specific measures adopted on the protection of minors or specific groups of data subjects;

d) The establishment of a seal of quality identifying subscribers to the code.

ARTICLE 75. GUARANTEES OF COMPLIANCE WITH CODES OF CONDUCT.

1. The codes of conduct shall include independent supervision procedures to guarantee compliance with the obligations assumed by subscribers, and to establish adequate, effective and dissuasive penalties.

2. Such procedure shall guarantee:

a) The independence and impartiality of the supervisory body;

b) The simple, accessible, fast and cost-free presentation of complaints and claims before the body for possible breaches of the code of conduct;

c) The right to contest;

d) Various levels of penalties so they may be adjusted to the severity of the breach. Such penalties shall be dissuasive and may involve suspension of the subscription to the code or expulsion from the member entity. If appropriate, it may establish its publication;

e) Notification of the decision taken to the data subject.

3. Similarly, and without prejudice to the provisions of Article 19 of Organic Law 15/1999, of 13 December, the codes of conduct may include procedures to determine measures to repair harm that may have been caused to data subjects as a result of the breach of the code of conduct.

4. These provisions of this Article shall be applied without prejudice to the powers of the Spanish Data Protection Agency and, if appropriate, of the supervisory authorities of the Autonomous Communities.

ARTICLE 76. LIST OF SUBSCRIBERS.

The code of conduct shall have attached as a schedule a list of subscribers, which shall be kept up-to-date, available to the Spanish Data Protection Agency.

ARTICLE 77. FILING AND PUBLICATION OF CODES OF CONDUCT.

1. In order for the codes of conduct to be considered as such for the purposes provided in Article 32 of Organic Law 15/1999, of 13 December, and herein, they shall be filed and registered in the General Data Protection Register of the Spanish Data Protection Agency or, when appropriate, in the register created by the Autonomous Communities, which shall transfer them for their inclusion in the General Data Protection Register.

2. For this purpose, the codes of conduct shall be presented before the relevant supervisory authority, that shall process their registration, in the event they are subject to the decision of the Spanish Data Protection Agency, pursuant to the procedure established in Chapter VI of Title IX hereof.

3. In any case, the Spanish Data Protection Agency shall publish the registered codes of conduct, preferably through computerised or telematic means.

ARTICLE 78. OBLIGATIONS AFTER REGISTRATION OF THE CODE OF CONDUCT.

The promoting entities or bodies, persons or entities designated for this purpose in the code of conduct shall have, once it has been published, the following obligations:

a) Maintain accessible to the public the updated information on the promoting entities, the content of the code of conduct, the procedures for subscription and guarantee of compliance and the list of subscribers to which the previous Article refers.

   Such information shall be presented clearly and concisely and shall be permanently accessible by electronic means.

b) Send to the Spanish Data Protection Agency an annual report on the activities carried out to disseminate the code of conduct and promote subscription to it, the actions for verifying compliance with the code and their results, the complaints and claims handled and the process they have undergone and any other aspect that the promoting entities deem relevant.

   Regarding codes of conduct registered in the register of a supervisory authority of an Autonomous Community, the report shall be sent to that authority, which shall transfer it to the General Data Protection Register.

c) Periodically evaluate the effectiveness of the code of conduct, measuring the degree of satisfaction of the data subjects and, if appropriate, updating the contents to adapt it to the general or sectoral legislation on the protection of data that is in force at any time.

   This evaluation shall take place, at least, every four years, unless adaptation of the commitments of the code to an amendment of the applicable legislation is required earlier.

d) Promote accessibility of all persons, paying particular attention to those with a disability or of advanced age, to the information available on the code of conduct.

TITLE VIII
Regarding security measures in the processing of personal data

CHAPTER I
General provisions

ARTICLE 79. SCOPE.

Data controllers and data processors shall implement the security measures pursuant to the provisions of this Title, whatever may be the system of processing.

ARTICLE 80. LEVELS OF SECURITY.

There are three levels of applicable security measures for files and processing: basic, medium and high.

ARTICLE 81. APPLICATION OF THE LEVELS OF SECURITY.

1. All files or processing of personal data shall adopt the basic-level security measures.

2. The following files or processing of personal data shall also implement medium-level security measures, in addition to the basic-level security measures:

a) Those relating to criminal or administrative offences;

b) Those whose operation is subject to Article 29 of Organic Law 15/1999, of 13 December;

c) Those controlled by the tax administrations and relating to the exercise of the powers of taxation;

d) Those controlled by financial institutions for purposes related to the provision of financial services;

e) Those controlled by the Management Agencies and Common Services of the Social Security and relating to the exercise of their powers. Similarly, those controlled by the Mutual Funds for accidents at work and occupational illness associated with the Social Security;

f) Those containing a set of personal data that provide a definition of the characteristics or identity of citizens and which permit the evaluation of specific aspects of their identity or behaviour.

3. The following files or processing of personal data shall also implement high-level security measures, in addition to the basic- and medium-level measures:

a) Those referring to data on ideology, trade union membership, religion, beliefs, racial origin, health or sex life;

b) Those containing or referring to data collected for security forces without the consent of the data subjects;

c) Those containing data arising from acts of gender-based violence.

4. As well as the basic- and medium-level security measures, the high-level security measure contained in Article 103 hereof shall be applied to files controlled by operators providing electronic communications services to the public or that exploit public electronic communications networks with regard to traffic and location data.

5. The implementation of basic-level security measure shall be sufficient for files or processing or data on ideology, trade union membership, religion, beliefs, racial origin, health or sex life if:

a) The data are used for the sole purpose of carrying out a monetary transfer to organisations to which the data subjects are associated or are members of;

b) Regarding non-automated files or processing that incidentally contain such data that have no relation with its purpose.

6. Basic-level security measures may also be implemented in the files or processing that contain data relating to health, referring exclusively to the degree of disability or the simple declaration of the condition of disability of the data subject, for the purpose of fulfilling public duties.

7. The measures included in each of the aforesaid levels are the minimum that can be applied, without prejudice to the current specific regulations or legal provisions that may be applicable in each case or those adopted on the initiative of the data controller.

8. For the purposes of facilitating compliance with the provisions herein, when an information system has files or processing that, depending on their specific purpose or use, or on the nature of the data they contain, require the application of a level of security measures different to that of the main system, they may be separated from the latter, with the relevant level of security measures being applicable in each case and whenever the relevant data and users with access to them can be delimited, and this is recorded in the security document.

ARTICLE 82. DATA PROCESSOR.

1. When the data controller provides access to the data, to the supports that contain them or to the resources of the information system that processes them, for a data processor providing his services on the premises of the data controller this shall be recorded in the security document of the latter. The staff of the data processor shall commit themselves to the fulfilment of the security measures set out therein.

2. If the service is provided by the data processor on his own premises, outside those of the data controller, he shall draw up a security document under the terms required by Article 88 hereof or complete that already drafted, if appropriate, identifying the filing system or processing and the data controller and including the security measures that are to be implemented in relation to such processing.

3. In any case, access to the data by the data processor shall be subject to the security measures set out herein.

ARTICLE 83. PROVISION OF SERVICES WITHOUT ACCESS TO PERSONAL DATA.

The data controller shall adopt the adequate measures to limit access of staff to personal data, to the supports that contain them or to the resources of the information system, for the execution of tasks that do not involve the processing of personal data.

With regard to external personnel, the service provision contract shall expressly record the prohibition of access to the personal data and the obligation of confidentiality regarding the data that personnel may become aware of due to provision of the service.

ARTICLE 84. DELEGATION OF AUTHORISATIONS.

The authorisations in this Title that are attributed to the data controller may be delegated to the persons designated for this purpose. The security document shall record the persons able to grant such authorisations as well as those who are delegated. Under no circumstances shall such delegation imply a delegation of the liability corresponding to the data controller.

ARTICLE 85. ACCESS TO DATA THROUGH COMMUNICATION NETWORKS.

The applicable security measures for the access to personal data through communications networks, whether public or not, shall guarantee a level of security equivalent to that applicable to local access, pursuant to the criteria established in Article 80.

ARTICLE 86. WORKING PROCEDURE OUTSIDE THE PREMISES OF THE DATA CONTROLLER OR DATA PROCESSOR.

1. When the personal data are stored in portable devices or are processed outside the premises of the data controller or the data processor, the data controller shall necessarily give his prior authorisation, and in any case shall guarantee the level of security relevant to the type of file processed.

2. The authorisation to which the previous paragraph refers shall be recorded in the security document and may be established for a user or for a user profile and shall set out the duration of its validity.

ARTICLE 87. TEMPORARY FILING SYSTEMS OR WORKING COPIES OF DOCUMENTS.

1. Temporary filing systems or copies of documents that have been created exclusively for the execution of temporary or auxiliary tasks shall comply with the relevant level of security pursuant to the criteria established in Article 81.

2. All temporary filing systems or working copies thus created shall be erased or destroyed once they are no longer necessary for the purposes for which they were created.

CHAPTER II
Security document

ARTICLE 88. THE SECURITY DOCUMENT.

1. The data controller shall draw up a security document including the technical and organisational measures according to current legislation on security that shall be binding on the personnel with access to the information systems.

2. The security document shall be of general application to all the filing systems or processing, or individual for each filing system or processing. Different security documents may be drawn up grouping filing systems or processing according to the processing system used for their organisation, or bearing in mind the organisational criteria of the data controller. In any case, it shall be considered an internal document of the organisation.

3. The document shall contain, at least, the following aspects:

a) Scope of application of the document with detailed specifications of the protected resources;

b) Measures, regulations, protocols for action, rules and standards aimed at guaranteeing the level of security required herein;

c) Tasks and obligations of the staff in relation to the processing of personal data included in the filing system;

d) Structure of the filing systems with personal data and description of the information systems that process them;

e) Procedure of notification, management and response to incidents;

f) The procedures for making backup copies and recovery of the data in the automated filing systems or processing;

g) The measures that shall necessarily be adopted for the transport of the supports or documents, as well as for their destruction, or if appropriate, their re-use.

4. In the event of the medium- or high-level security measures provided in this Title being applicable to the filing systems, the security document shall also contain:

a) The identification of the data controller(s);

b) The monitoring that shall be carried out from time to time to verify fulfilment of that provided therein.

5. In the event of data processing by third parties, the security document shall contain the identification of the files or processing that have been commissioned with express reference to the contract or document regulating the conditions of the commission, as well as the identification of the data controller and the duration of validity of the commission.

6. In those cases where the personal data of a filing system or processing are included and processed exclusively in the systems of the data processor, the data controller shall record this in the security document. When this affects part or all of the filing systems or processing of the data controller, he shall delegate the security document to the data processor, with the exception of that relating to the data contained in his own resources. This fact shall be expressly indicated in the contract executed under Article 12 of Organic Law 15/1999, of 13 December, specifying the affected files or processing.

In this case, reference shall be made to the security document of the data processor for the purpose of fulfilment of that provided herein.

7. The security document shall be kept up-to-date at all times and shall be reviewed whenever any material changes are made to the information system, the processing system used, its organisation, the contents of the information included in the filing systems or processing or, if appropriate, as a result of the periodic monitoring. In any case, a change shall be deemed material when it may have repercussions on the fulfilment of the implemented security measures.

8. The content of the security document shall be adapted, at all times, to the current provisions of the security of personal data.

CHAPTER III
Security measures applicable to automated filing systems and processing

Section One. Basic-level security measures

ARTICLE 89. THE FUNCTIONS AND OBLIGATIONS OF STAFF.

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

The monitoring functions or authorisations delegated by the data controller of the filing system or processing shall also be defined.

2. The data controller shall adopt the necessary measures so that the staff members understand the security regulations that affect the performance of their functions as well as the consequences that may arise in the event of non-performance.

ARTICLE 90. RECORD OF INCIDENTS.

There shall be a procedure for notification and management of incidents that affect personal data and a register established for recording the type of incident, the moment it occurred, or if appropriate, was detected, the person making the notification, to whom it was communicated, the effect arising from it and the corrective measures applied.

ARTICLE 91. ACCESS CONTROL.

1. The users shall only have access to those resources required for the performance of their functions.

2. The data controller shall ensure there is an updated list of users and user profiles, and the authorised accesses for each one.

3. The data controller shall establish mechanisms to avoid a user being able to access resources with rights other than those authorised.

4. Only staff members authorised in the security document shall grant, alter or annul the access authorised to resources, pursuant to the criteria established by the data controller.

5. Should personnel not pertaining to the data controller have access to the resources they shall be subject to the same security conditions and obligations as the internal personnel.

ARTICLE 92. MANAGEMENT OF SUPPORTS AND DOCUMENTS.

1. The supports and documents containing personal data shall permit identification of the type of information they contain, allow an inventory to be taken and shall only be accessible by the personnel authorised in the security document.

An exception to these obligations shall be made when the physical characteristics of the support makes their fulfilment impossible, a record justifying this fact being made in the security document.

2. The departure of supports and documents containing personal data, including those comprising and/or attached to e-mails, outside the premises under the control of the data controller shall be authorised by the data controller or be duly authorised in the security document.

3. Measures aimed at avoiding the theft, loss or unauthorised access to the information during transport shall be taken in the transfer of documentation.

4. Any document or support containing personal data that is to be discarded shall always be erased or destroyed , by taking measures aimed at avoiding access to the information contained therein or its later recovery.

5. The identification of the supports containing personal data that the organisation deems particularly sensitive may be made using logical labelling systems permitting authorised users of such supports and documents to identify their content, and making identification difficult for anyone else not so authorised.

ARTICLE 93. IDENTIFICATION AND AUTHENTICATION.

1. The data controller shall take the measures that guarantee the correct identification and authentication of the users.

2. The data controller shall establish a mechanism that permits the unequivocal and personalised identification of any user who tries to access the information system and the verification of his authorisation.

3. When the authentication mechanism is based on the existence of passwords there shall be a procedure of disclosure, distribution and storage guaranteeing their confidentiality and integrity.

4. The security document shall establish the frequency, which under no circumstances shall be less than yearly, with which the passwords shall be changed. Whilst in force, passwords shall be stored in an unintelligible way.

ARTICLE 94. BACKUP COPIES AND RECOVERY.

1. Protocols for action shall be established for making weekly backup copies, at least, unless data have been updated during that time.

2. Similarly, procedures for the recovery of data shall be established to guarantee at all times their reconstruction to the original state at the moment the loss or destruction occurred.

Manual recording of the data shall only be done when the loss or destruction affects partially automated filing systems or processing, and whenever the existence of documentation allows

for the objective to be met to which the previous paragraph refers; a justified record of this fact being made in the security document.

3. The data controller shall ensure verification every six months of the correct definition, operation and application of the procedures for making backup copies and for the recovery of data.

4. The tests prior to the implementation or amendment of the information systems the process filing systems with personal data shall not be done with real data, unless the relevant level of security for the processing is ensured and it is recorded in the security document.

If tests are to be done with real data, a backup copy shall be made first.

Section Two. Medium-level security measures

ARTICLE 95. SECURITY OFFICER.

The security document shall appoint one or several security officers commissioned with co-ordinating and monitoring the measures defined therein. This appointment may be general for all the filing systems or processing of personal data or specific depending on the information systems used, which shall be clearly recorded in the security document.

Under no circumstances shall this designation imply an exemption of the liability corresponding to the data controller or data processor pursuant to this Regulation.

ARTICLE 96. AUDIT.

1. At the medium and higher levels the information systems and processing and data storage installations shall be subject, at least every two years, to an internal or external audit that verifies compliance with this Title.

In extraordinary circumstances the audit shall be done whenever substantial amendments to the information system are made that may have repercussions in the fulfilment of the implemented security measures for the purpose of verifying their adaptation, adjustment and efficiency. This audit starts the calculation of the aforesaid two years.

2. The audit report shall report on the adaptation of the measures and monitoring to the Law and its regulations, identifying deficiencies and proposing the necessary corrective or complementary measures. It shall also include the data, facts and observations on which the reports are based and recommendations proposed.

3. The audit reports shall be analysed by the competent security officer, who shall inform the data controller of the conclusions so he may take the adequate corrective measures and they shall be made available to the Spanish Data Protection Agency or, if appropriate, the supervisory authorities of the Autonomous Communities.

ARTICLE 97. MANAGEMENT OF SUPPORTS AND DOCUMENTS.

1. A registration system for the entry of supports shall be established permitting, directly or indirectly, the type of document or support to be known, as well as the date and time, the issuer, the number of documents or supports included in the despatch, the type of information they contain, the method of despatch and the person responsible for receipt, who shall be duly authorised.

2. Similarly, a registration system for the departure of supports shall be provided permitting, directly or indirectly, the type of document or support to be known, as well as the date and time, the recipient, the number of documents or supports included in the despatch, the type of information they contain, the method of despatch and the person responsible for delivery, who shall be duly authorised.

ARTICLE 98. IDENTIFICATION AND AUTHENTICATION.

The data controller shall establish a mechanism to limit the possibility of repeated attempts of unauthorised access to the information systems.

ARTICLE 99. PHYSICAL ACCESS CONTROL.

Only the personnel authorised in the security document shall have access to the places housing the physical equipment that supports the information systems.

ARTICLE 100. RECORD OF INCIDENTS.

1. The register regulated in Article 90 shall also provide the procedures for the recovery of data, indicating the person who executed the process, the data restored and, if appropriate, which data have had to be manually recorded in the recovery process.
2. Authorisation of the data controller shall be necessary for the execution of the data recovery procedures.

Section Three. High-level security measures

ARTICLE 101. MANAGEMENT AND DISTRIBUTION OF MEDIA.

1. The identification of the supports shall be done using logical labelling systems allowing users with authorised access to such supports and documents to identify their contents, and making identification difficult for everyone else.

2. The distribution of supports containing personal data shall be done encoding such data or using another mechanism that guarantees that such information is not accessible or manipulated during transport.

Similarly, the data contained in portable devices shall be encoded when they are outside the installations of the data controller.

3. The processing of personal data in portable devices that do not permit encoding shall be avoided. Should it be strictly necessary it shall be recorded with the justification in the security document and measures shall be taken bearing in mind the risks of processing in unprotected environments.

ARTICLE 102. BACKUP COPIES AND RECOVERY.

A backup copy of the data and of their recovery procedures shall be kept in a different place to that housing the computer equipment that processes them, which shall in any case comply with the security measures required herein, or use elements that guarantee the integrity and recovery of the information, so that their recovery is possible.

ARTICLE 103. ACCESS RECORD.

1. For each attempt at access at least the following shall be stored: identification of the user, the date and time it was done, the filing system accessed, the type of access and whether it has been authorised or denied.

2. Should access be authorised, it shall be necessary to store the information allowing the accessed register to be identified.

3. The mechanisms that permit the register of accesses shall be under the direct control of the competent security officer and shall not permit their deactivation or manipulation.

4. The minimum period for storing the registered data shall be two years.

5. The security officer shall review the registered monitoring information at least once a month and shall draft a report of the revisions and the problems detected.

6. The registration of accesses defined herein shall not be necessary when the following circumstances concur:

a) The data controller is a natural person;

b) The data controller guarantees that only he has access and processes the personal data.

The concurrence of these aforesaid circumstances shall be expressly recorded in the security document.

ARTICLE 104. TELECOMMUNICATIONS.

When, pursuant to Article 81.3, the high-level security measures must be implemented, the transfer of personal data through public or wireless electronic communications networks shall be done encoding such data or using any other mechanism that guarantees the information shall not be intelligible or manipulated by third parties.

CHAPTER IV

Security measures applicable to non-automated filing systems and processing

Section One. Basic-level security measures.

ARTICLE 105. COMMON OBLIGATIONS.

1. In addition to the provisions of this Chapter, the provisions of Chapters I and II of this Title shall be applicable to non-automated files relating to:

a) Scope

b) Levels of security

c) The data processor

d) Provisions of services without access to personal data

e) Delegation of authorisations

f) Working procedure outside the premises of the data controller or data processor

g) Working copies of documents

h) The security document.

2. The provisions established in section one of Chapter III of this Title shall also be applicable relating to:

a) Functions and obligations of staff members

b) Register of incidents

c) Control of access

d) Management of supports.

ARTICLE 106. FILING CRITERIA.

The filing of supports or documents shall be done pursuant to the criteria set out in the respective legislation. Such criteria shall guarantee the correct storage of the documents, the location and consultation of the information and allow the exercise of the rights of objection to the processing, access, rectification and erasure.

Should there not be any applicable regulation, the data controller shall establish the criteria and protocols for action that must be followed for the filing.

ARTICLE 107. STORAGE DEVICES.

The storage devices for the documents containing personal data shall have mechanisms that hinder opening. When their physical characteristics do not permit such a measure, the data controller shall adopt the measures that prevent access by unauthorised persons.

ARTICLE 108. SAFEKEEPING OF MEDIA.

Whilst the documentation containing personal data is not filed in the storage devices established above, due to undergoing revision or processing, whether before or after their filing, the person who is responsible for them shall ensure their safekeeping and prevent at all times their access by unauthorised persons.

Section Two. Medium-level security measures

ARTICLE 109. RESPONSIBILITY FOR SECURITY.

One or several security officers shall be designated under the terms and with the functions set out in Article 95 hereof.

ARTICLE 110. AUDIT.

The filing systems comprising this section shall be subject to an internal or external audit, at least every two years, which verifies compliance with this Title.

Section Three. High-level security measures

ARTICLE 111. STORAGE OF INFORMATION.

1. The cupboards, filing cabinets or other elements for storing non-automated files with personal data shall be in areas to which access is protected by entrance doors with locks or another equivalent device. Such areas shall remain closed when access to the documents included in the filing system is not required.

2. If, bearing in mind the characteristics of the premises available to the data controller, it is not possible to comply with that provided above, the data controller shall adopt alternative measures that, duly justified, shall be included in the security document.

ARTICLE 112. COPY OR REPRODUCTION.

1. The generation of copies or the reproduction of the documents shall only be done under the control of the personnel authorised in the security document.

2. Copies or reproductions to be discarded shall be destroyed to avoid access to the information contained therein or its later recovery.

ARTICLE 113. ACCESS TO DOCUMENTS.

1. Access to the documentation shall be exclusively limited to the authorised personnel.

2. Mechanisms shall be established to permit identification of access to documents that may be used by multiple users.

3. The access of persons not included above shall be adequately registered pursuant to the procedure established for this purpose in the security document.

ARTICLE 114. TRANSFER OF DOCUMENTS.

Whenever there is a physical transfer of the documentation contained in a filing system, measures shall be adopted aimed at preventing access or manipulation of the information being transferred.

TITLE IX
Procedures handled by the Spanish Data Protection Agency

CHAPTER I
General provisions

ARTICLE 115. APPLICABLE SYSTEM.

1. The procedures handled by the Spanish Data Protection Agency shall be subject to the provisions of this Title and, in addition, to Act 30/1992, of 26 November, of the Regulation of the Public Administrations and the Common Administrative Procedure.

2. The regulations of the common administrative procedure shall be specifically applicable to the system of representation in such procedures.

ARTICLE 116. PUBLICATION OF RESOLUTIONS.

1. The Spanish Data Protection Agency shall publish its resolutions, with the exception of those relating to the registration of a filing system or processing in the General Data Protection Register and those settling the registration therein of the codes of conduct, whenever they refer to procedures started after 1 January 2004, or that correspond to the filing of inspections initiated after this date.

2. The publication of these resolutions shall preferably be done by their insertion on the website of the Spanish Data Protection Agency, within one month of the date of their notification to data subjects.

3. The notification of resolutions shall expressly inform data subjects of the publication requirements set out in Article 37.2 of Organic Law 15/1999, of 13 December.

4. The publication shall be done applying the dissociation criteria of the personal data that are established for this purpose by Decision of the Director of the Agency.

CHAPTER II

Procedure for the protection of the rights of access, rectification, erasure and objection

ARTICLE 117. INVESTIGATION INCIDENT TO THE PROCEDURE.

1. The procedure shall be initiated at the request of the data subject(s), clearly expressing the content of their claim and of the provisions of Organic Law 15/1999, of 13 December, they consider breached.

2. Once the Spanish Data Protection Agency has received the claim, it shall transfer it to the data controller, so that, within fifteen days, he may lodge any pleading he deems appropriate.

3. Having received the pleading or the aforesaid time limit having expired, the Spanish Data Protection Agency shall settle the submitted claim, in view of the reports, evidence and other relevant acts of investigation, including a hearing with the data subject and again with the data controller.

ARTICLE 118. DURATION OF THE PROCEDURE AND EFFECTS OF THE ABSENCE OF A DECISION.

1. The maximum time limit for issuing and notifying a decision in the procedure for the protection of rights shall be six months, starting from the date of entry in the Spanish Data Protection Agency of the claim of the data subject(s).

2. If a decision has not been issued and notified within this time, the data subject may consider his claim upheld due to affirmative administrative silence.

ARTICLE 119. EXECUTION OF THE DECISION.

If the decision for protection is in favour, the data controller shall be given notice so that, within ten days following the notification, he shall make effective the exercise of the rights subject to protection, having to necessarily provide written evidence of compliance with the Spanish Data Protection Agency within the same period of time.

CHAPTER III

Procedures relating to exercising the power to impose penalties

Section One. General provisions.

ARTICLE 120. SCOPE OF APPLICATION.

1. The provisions contained in this Chapter shall be applicable to the procedures relating to the exercise by the Spanish Data Protection Agency of the power to impose penalties, in application of the provisions of Organic Law 15/1999, of 13 December, on the protection of personal data, of Act 34/2002, of 11 July, on Information Society Services and Electronic Commerce and of the State Telecommunications Act 32/2003, of 3 November.

2. The aforesaid notwithstanding, the provisions of Article 121 and of section four of this Chapter shall only be applicable to those procedures referring to the exercise of the power to impose penalties provided in Organic Law 15/1999, of 13 December.

ARTICLE 121. BLOCKING OF FILES.

1. In the event of a very serious breach provided in Organic Law 15/1999, of 13 December, comprising the illicit use or disclosure of the personal data that seriously prevents or threatens the exercise of the rights of citizens and the free development of identity guaranteed by the Constitution and the law, the Director of the Spanish Data Protection Agency may, at any time during the procedure, demand of the data controller of personal data, whether publicly- or privately-owned, the cessation of the illicit use or disclosure of the data.

2. The demand shall be necessarily executed within a maximum period of three days, during which the data controller shall lodge any pleading he deems appropriate in order to lift the measure.

3. If the demand is ignored, the Director of the Spanish Data Protection Agency may, following an argued decision, decide to block such files or processing, for the sole purpose of restoring the rights of the data subjects.

Section Two. Preliminary proceedings

ARTICLE 122. INITIATION.

1. Prior to the initiation of the sanction procedure, preliminary proceedings may be instigated for the purpose of determining whether the circumstances justify their initiation. In particular, these proceedings shall be aimed at determining, as precisely as possible, the facts that may justify the instigation of the proceedings, identify the person or body that may be liable and setting out the relevant circumstances that may apply.

2. The preliminary proceedings shall be carried out ex- officio by the Spanish Data Protection Agency, either at its own initiative or as a result of a complaint or reasoned request from another body.

3. When the proceedings are the result of a complaint or reasoned request from another body, the Spanish Data Protection Agency shall acknowledge receipt of the complaint or request,

asking for any documentation it deems relevant to be able to verify the facts capable of justifying the instigation of the sanction procedure.

4. These preliminary proceedings shall have a maximum duration of twelve months starting from the date the complaint or reasoned request to which subsection 2 refers enters the Spanish Data Protection Agency or, if these do not exist, from the date the Director of the Agency resolves to commence such proceedings.

Expiry of the period without the issue and notification of the resolution to initiate the sanction procedure shall result in the expiry of the preliminary proceedings.

ARTICLE 123. COMPETENT STAFF FOR CARRYING OUT PRELIMINARY PROCEEDINGS.

1. Preliminary proceedings shall be carried out by staff members of the Data Inspection Department members who are qualified for the exercise of inspection tasks.

2. In exceptional situations, the Director of the Spanish Data Protection Agency may appoint to undertake specific tasks those officials of the Agency who are not generally qualified for the exercise of inspection tasks or civil servants who do not provide services in the Agency, whenever they comply with the necessary conditions of suitability and specialisation for carrying out such proceedings. In these cases, the authorisation shall expressly indicate the identification of the civil servant and the specific preliminary inspection proceedings to be done.

3. The employees who carry out the inspection to which the two previous subsections refer shall be considered a public authority for the performance of their tasks.

They shall be bound to keep secret any information of which they become aware in the exercise of the aforesaid functions, even after they have ceased in the exercise thereof.

ARTICLE 124. OBTAINING INFORMATION.

The inspectors may collect any information required for the performance of their tasks. For this purpose they may demand the exhibition or despatch of the documents and data and examine them where they are filed, obtain a copy of them, inspect the physical equipment and software, as well as demand the execution of processing and management programmes and procedures and support of the filing system or filing systems subject to investigation, accessing the locations where they are installed.

ARTICLE 125. ON-SITE INSPECTIONS.

1. In the performance of the preliminary proceedings the designated inspectors may make inspections in the premises or headquarters of the inspected party, or wherever the filing systems are located, if appropriate. For this purpose, the inspectors shall have been previously authorised by the Director of the Spanish Data Protection Agency.

Inspections may take place in the domicile of the inspected party, in the headquarters or specific premises related with it or in any of its premises, including those where the processing is done by a commissioned party.

The authorisation shall be limited to indicating the entitlement of the authorised inspector and the identification of the person or body inspected.

2. In the situation contemplated above, the inspections shall conclude with the issue of the relevant document that records the proceedings carried out during the inspection(s).

3. The document, issued in two counterparts, shall be signed by the acting inspectors and the inspected party, which may record therein the pleadings or statements deemed appropriate.

Should the inspected party refuse to sign the document, this shall be expressly recorded therein. In any case, the signature of the document by the inspected party shall not imply agreement with it, only its receipt.

The inspected party shall be handed one of the originals of the inspection document, and the other shall be added to the proceeding records.

ARTICLE 126. OUTCOME OF PRELIMINARY PROCEEDINGS.

1. Once the preliminary proceedings have ended, these shall be subject to the decision of the Director of the Spanish Data Protection Agency.

If the proceedings do not result in any indications justifying the charge of a breach, the Director of the Spanish Data Protection Agency shall issue a resolution for the record that shall be notified to the investigated party and the complainant, as may be the case.

2. Should there be indications justifying the charge of a breach, the Director of the Spanish Data Protection Agency shall issue a resolution to initiate the sanction or infringement procedure of the public administrations, which shall be processed pursuant to that provided, respectively, in sections three and four of this Chapter.

Section Three. Sanction procedure

ARTICLE 127. INITIATION OF THE PROCEDURE.

The resolution to initiate the sanction procedure shall specifically contain:

a) Identification of the person or persons allegedly responsible;

b) A succinct description of the charges, their possible qualification and the penalties that may correspond, without prejudice to that resulting from the investigation;

c) Indication that the competent body for the procedure is the Director of the Spanish Data Protection Agency;

d) Indication to the alleged person responsible that he may voluntarily acknowledge his responsibility, in which case a decision shall be issued forthwith;

e) Designation of an investigator and, if appropriate, secretary, with express indication of their rules governing challenges;

f) Express indication of the right of the person responsible to lodge pleadings, to a hearing in the proceedings and to propose the evidence he deems relevant;

g) The provisional measures that may be ordered, if appropriate, pursuant to that established in section one of this Chapter.

ARTICLE 128. MAXIMUM TIME LIMIT FOR DECISION.

1. The deadline for issuing a decision shall be that set out in the regulations applicable to each penalty procedure and shall be calculated from the date the resolution to initiate is issued until the notification of the penalty occurs, or the attempt of notification is duly accredited.

2. The expiry of the aforesaid maximum period, without a decision being issued and notified, shall result in the expiry of the procedure and the filing of the proceedings.

Section Four. Procedure for declaring a breach of Organic Law 15/1999, of 13 December, by Public Administrations.

ARTICLE 129. GENERAL PROVISION.

The procedure for declaring a breach of Organic Law 15/1999, of 13 December by the public administrations shall be the provisions of section three of this Chapter.

CHAPTER IV
Procedures relating to the registration or erasure of filing systems

Section One. Procedure for registering the creation, amendment or deletion of filing systems

ARTICLE 130. INITIATION OF THE PROCEDURE.

1. The procedure shall be initiated as a result of the notification of the creation, amendment or deletion of the filing system by the data subject or, if appropriate, of the communication made by the supervisory authorities of the Autonomous Communities, to which this Regulation refers.

2. The notification shall be made by filling in the electronic models or forms published for this purpose by the Spanish Data Protection Agency, by virtue of the provisions of Article 59(1) hereof.

The notification of the amendment or deletion of a filing system shall indicate therein the registration code of the file in the General Data Protection Registry.

3. The notification shall be done on an electronic support, through electronic communication via the Internet either by electronic signature or on a computer support, using the 'Help' program for this purpose to generate notifications that the Agency shall make available to data subjects free of charge.

Notification on paper shall be equally valid when the models or forms published by the Agency have been used.

4. In such notification, the data controller shall declare an address for notification purposes during the procedure.

ARTICLE 131. SPECIAL PROVISIONS IN THE NOTIFICATION OF PUBLICLY-OWNED FILING SYSTEMS.

1. With regard to the notification of publicly-owned filing systems, it shall be accompanied by a copy of the provision or resolution of creation, amendment or deletion of the filing system to which Article 52 hereof refers.

When the Official Spanish Gazette in which the aforesaid provision or resolution is published is accessible via Internet, it shall be sufficient for the notification to contain the URL permitting its specific location.

2. Having received the notification, if it does not contain the mandatory information or formal defects are detected, the General Data Protection Registry shall ask the data controller to complete or remedy the notification, The deadline for the remedy or improvement of the request shall be three months, should the amendment of the provision or resolution of creation of the filing system be required.

ARTICLE 132. RESOLUTION FOR REGISTRATION OR ERASURE.

If the notification referring to the creation, amendment or deletion of the filing system contains the mandatory information and the other legal requirements are met, the Director of the Spanish Data Protection Agency, at the proposal of the General Data Protection Registry, shall decide, respectively, the registration of the filing system, assigning it the relevant registration code, the amendment of the registration of the filing system or the erasure of the relevant entry.

ARTICLE 133. ILLEGALITY OR DENIAL OF REGISTRATION.

The Director of the Spanish Data Protection Agency, at the proposal of the General Data Protection Registry, shall issue a decision denying the registration, amendment or erasure when the documents provided by the data controller show that the notification is not pursuant to the provisions of Organic Law 15/1999, of 13 December.

The decision shall be duly argued, with express indication of the causes preventing the registration, rectification or erasure.

ARTICLE 134. DURATION OF THE PROCEDURE AND EFFECTS OF THE LACK OF A DECISION.

1. The maximum period for issuing and notifying the decision regarding the registration, amendment or erasure shall be one month.

2. If in this time a decision has not been issued and notified, the filing system shall be deemed registered, modified or erased for all legal purposes.

Section Two. Procedure for ex- officio erasure of registered filing system

ARTICLE 135. INITIATION OF THE PROCEDURE.

The procedure for the ex- officio erasure of the filing system registered in the General Data Protection Registry shall always be initiated ex- officio, either by its own initiative or by virtue of a complaint, by resolution of the Director of the Spanish Data Protection Agency.

ARTICLE 136. TERMINATION OF THE PROCEDURE.

The decision, following a hearing with the data subject, shall resolve to give rise or not to the erasure of the filing system.

If the decision resolves to erase the filing system, it shall be notified to the General Data Protection Registry, so it may proceed with the erasure.

CHAPTER V
Procedures regarding international data transfers

Section One. Authorisation procedure for international data transfers.

ARTICLE 137. INITIATION OF THE PROCEDURE.

1. The procedure for obtaining the authorisation for the international data transfers to third countries to which Article 33 of Organic Law 15/1999, of 13 December, and Article 70 hereof refer, shall always be initiated at the request of the exporter that intends to carry out the transfer.

2. In addition to the legally enforceable requirements, the exporter shall set out in his request, in all cases:

a) The identification of the filing system or filing systems containing data to which the international transfer refers, indicating the name and registration code of the filing system in the General Data Protection Registry;

b) The transfer or transfers for which he requests authorisation, indicating the purpose that justifies it/them;

c) The documentation including the applicable guarantees for obtaining the authorisation as well as compliance with the legal requirements necessary for the realisation of the transfer, if appropriate.

When the authorisation is founded on the existence of a contract between the data exporter and the data importer, a copy shall be provided and evidence shall also be provided of the sufficient power of its parties.

If the authorisation intends to be founded on the provisions of Article 70(4), the provisions or rules adopted in relation to the processing of data within the group shall be provided, as well as the documentation that accredits its binding nature and effectiveness within the group. Similarly, the documentation that confirms the possibility that the data subject or the Spanish Data Protection Agency may demand the relevant liability in the event of harm to the data subject or breach of the data protection laws by any importing company shall be provided.

ARTICLE 138. CARRYING OUT OF THE PROCEDURE.

1. When the Director of the Spanish Data Protection Agency decides, pursuant to the provisions of Article 86.1 of Act 30/1992, of 26 November, the start of a period of public information, the period for lodging pleadings shall be ten days starting from the publication in the Official Spanish Gazette of the announcement required by the Act.

2. Access to the information of the filing system shall not be permissible where the circumstances established in Article 37.5 of Act 30/1992, of 26 November concur.

3. On expiry of the time limit provided in subsection 1, should pleadings have been made, they shall be notified to the person requesting authorisation, so that within ten days he may provide the arguments he deems relevant.

ARTICLE 139. ACTIONS AFTER THE DECISION.

1. When the Director of the Spanish Data Protection Agency decides to authorise the international transfer of data, the decision for authorisation shall be notified to the General Data Protection Registry for its registration.

The General Data Protection Registry shall register ex- officio the authorisation of the international transfer.

2. In any case, the decision for authorisation or denial of the authorisation for the international transfer of data shall be notified to the Ministry of Justice, for the purpose of its notification to

the European Commission and the other Member States of the European Union pursuant to the provisions of Article 26.3 of Directive 95/46/EC.

ARTICLE 140. DURATION OF THE PROCEDURE AND EFFECTS OF THE LACK OF A DECISION.

1. The maximum period for issuing and notifying the decision shall be three months, starting from the date of entry in the Spanish Data Protection Agency of the request.

2. If in this time a decision has not been issued and notified, the international transfer of data shall be deemed authorised.

Section Two. Procedure for the temporary suspension of international data transfers

ARTICLE 141. INITIATION.

1. In the situations included in Article 69 and Article 70(3), the Director of the Spanish Data Protection Agency may decide the temporary suspension of an international transfer of data.

2. In such situations, the Director shall issue a resolution of initiation referring to the temporary suspension of the transfer. The resolution shall be justified and founded in the provisions of this Regulation.

ARTICLE 142. INVESTIGATION AND DECISION.

1. The resolution shall be notified to the data exporter, so that within fifteen days he may provide the arguments he deems relevant.

2. Having received the arguments or on expiry of the time limit, the Director shall issue a decision deciding, if appropriate, the temporary suspension of the international transfer of data.

ARTICLE 143. ACTIONS AFTER THE DECISION.

1. The Director of the Spanish Data Protection Agency shall notify the decision to the General Data Protection Registry so it may be recorded therein.

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

2. In any case, the decision shall be notified to the Ministry of Justice, for the purpose of its notification to the European Commission and the other Member States of the European Union 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 reasons justifying its imposition have ceased, following a decision of the Director of the Spanish Data Protection Agency, which shall be notified to the data exporter.

2. The Director of the Spanish Data Protection Agency shall notify the decision to the General Data Protection Registry so it may be recorded therein.

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

3. The resolution shall be notified to the data exporter and the Ministry of Justice, for the purpose of its notification to the European Commission and the other Member States of the European Union pursuant to the provisions of Article 26.3 of Directive 95/46/EC.

CHAPTER VI
Registration procedure for codes of conduct

ARTICLE 145. INITIATION OF THE PROCEDURE.

1. The procedure for registration in the General Data Protection Registry of the codes of conduct shall always be initiated at the request of the promoting entity, body or association of the code of conduct.

2. The request, which shall comply with the legally established requirements, shall be accompanied by the following documents:

a) Accreditation of the representation applying to the person presenting the request.

b) Contents of the resolution or decision that approves the content of the presented code of conduct, within the relevant scope.

c) Should the code of conduct arise from a sectoral agreement or a decision of the company, a certificate regarding the adoption of the agreement and legitimacy of the body adopting it.

d) In the event of that provided above, a copy of the Articles of Association, sectoral organisation or entity approving the code.

e) For codes of conduct presented by sectoral associations or organisations, documentation relating to its representation of the sector.

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

g) Code of conduct submitted to the Spanish Data Protection Agency.

ARTICLE 146. ANALYSIS OF THE SUBSTANTIVE ASPECTS OF THE CODE OF CONDUCT.

1. During the thirty days following notification or remedy of the defects the General Data Protection Registry shall convene those making the request, in order to obtain clarifications or details relating to the substantive content of the code of conduct.
2. On expiry of the time limit stated above, the General Data Protection Registry shall draft a report on the characteristics of the code of conduct proposal.

3. The presented documentation and the report from the Registry shall be sent to the Legal Department, so that it may inform on compliance with the requirements established in Title VIII hereof.

ARTICLE 147. PUBLIC INFORMATION.

1. When the Director of the Spanish Data Protection Agency decides, pursuant to the provisions of Article 86.1 of Act 30/1992, of 26 November, to start a period of public information, the period for lodging pleadings shall be ten days starting from the publication in the Official Spanish Gazette of the announcement required by the Act.

2. Access to the information of the file shall not be possible where the circumstances established in Article 37.5 of Act 30/1992, of 26 November concur.

ARTICLE 148. IMPROVEMENT OF THE CODE OF CONDUCT.

If during the procedure the provision of new documents is necessary or amendment of the presented code of conduct, the Spanish Data Protection Agency may request this of the applicant, so that within thirty days he enters the relevant amendments, sending the resulting text to the Spanish Data Protection Agency. The suspension of the procedure shall be declared if the applicant does not comply with the request.

ARTICLE 149. PERIOD FOR COMMENTS.

If during the procedure provided in Article 148 any pleading have been made, they shall be notified to the person requesting authorisation, so that within ten days he may provide the arguments he deems relevant.

ARTICLE 150. DECISION.

1. Having complied with the terms established in the preceding Articles, the Director of the Agency shall make a decision on the legality or illegality of the registration of the code of conduct in the General Data Protection Registry.

2. When the Director of the Spanish Data Protection Agency decides to authorise the registration of the code of conduct, the decision shall be notified to the General Data Protection Registry for its registration.

ARTICLE 151. DURATION OF THE PROCEDURE AND EFFECTS OF THE LACK OF A DECISION.

1. The maximum time limit for issuing and notifying a decision shall be six months, starting from the date of entry of the request in the Spanish Data Protection Agency.

2. If a decision has not been issued and notified within this time, the person making the request may consider it accepted.

ARTICLE 152. PUBLICATION OF THE CODES OF CONDUCT BY THE SPANISH DATA PROTECTION AGENCY.

The Spanish Data Protection Agency shall publish the content of the codes of conduct registered in the General Data Protection Registry, preferably using electronic or telematic means.

CHAPTER VII
Other procedures handled by the Spanish Data Protection Agency

Section One. Procedure for exemption of the duty of information to the data subject.

ARTICLE 153. INITIATION OF THE PROCEDURE.

1. The procedure to obtain from the Spanish Data Protection Agency the exemption from the duty to inform the data subject of the processing of his personal data when this is impossible or requires disproportionate efforts, provided in Article 5/5) of Organic Law 15/1999, of 13 December, shall always be initiated at the request of the data controller who wishes to obtain application of the exemption.

2. In addition to the requirements set out in Article 70 of Act 30/1992, of 26 November, in the written request the data controller shall:

a) Clearly identify the data processing to which he wishes the exemption from the duty to inform to apply;

b) Expressly justify the reasons on which the impossible nature or disproportionate nature of the effort implied by compliance with the duty to inform is founded;

c) List in detail the compensatory measures he proposes in the event of exemption from compliance with the duty to inform;.

d) Provide informative statement that, through its dissemination, under the terms indicated in the request, permits compensation of the exemption from the duty to inform.

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 decide to adopt measures complementing or substituting those proposed by him in the request.

2. The resolution shall be notified to the applicant, so he may make the statements he deems appropriate within fifteen days.

ARTICLE 155. TERMINATION OF THE PROCEDURE.

Having concluded the procedure provided above, the Director of the Agency shall issue a decision, granting or denying the exemption from the duty to inform. The decision may impose the adoption of the complementary measures to which the previous Article refers.

ARTICLE 156. DURATION OF THE PROCEDURE AND EFFECTS OF THE LACK OF A DECISION.

1. The maximum time limit for issuing and notifying a decision in the procedure shall be six months, starting from the date of entry in the Spanish Data Protection Agency of the request of the data controller.

2. If a decision has not been issued and notified within this time, the data controller may consider his request accepted due to affirmative administrative silence.

Section Two. Procedure to authorise the conservation of data for historical, statistical or scientific purposes.

ARTICLE 157. INITIATION OF THE PROCEDURE.

1. The procedure to obtain from the Spanish Data Protection Agency the declaration of the application for a specific processing of data for historical, scientific or statistical purposes, for the purposes provided in Organic Law 15/1999, of 13 December, and herein, shall always be initiated at the request of the data controller who wishes to obtain the declaration.

2. In the written request the data controller shall:

a) Clearly identify the data processing to which he wishes to apply the exception;

b) Expressly state the reasons that would justify the declaration;

c) List in detail the compensatory measures he proposes to implement to guarantee the citizens' rights.

3. The request shall be accompanied by any documents or other evidence necessary to justify the existence of the historical, scientific or statistical values that would be the basis of the declaration by the Agency.

ARTICLE 158. DURATION OF THE PROCEDURE AND EFFECTS OF THE LACK OF A DECISION.

1. The maximum time limit for issuing and notifying a decision in the procedure shall be three months, starting from the date of entry in the Spanish Data Protection Agency of the request of the data controller.

2. If a decision has not been issued and notified within this time, the data controller may consider his request accepted.

SOLE ADDITIONAL PROVISION. SOFTWARE PRODUCTS.

The software products destined for the automated processing of personal data shall include in their technical description the level of security, basic, medium or high, they can attain in accordance with the provisions of Title VIII hereof.

SOLE FINAL PROVISION. SUPPLEMENTARY LAW.

Insofar as not specified in Chapter III of Title IX the provisions contained in the Procedural Regulation for the exercise of the authority to impose penalties, approved by Royal Decree 1398/1993, of 4 August, shall be applicable to the penalty procedures processed by the Spanish Data Protection Agency.