PERSONAL DATA PROTECTION CODE

Legislative Decree no. 196 dated 30 June 2003

THE PRESIDENT OF THE REPUBLIC

HAVING REGARD to Articles 76 and 87 in the Constitution,

HAVING REGARD to Section 1 of Act no. 127 of 24 March 2001, enabling Government to issue a consolidated text on the processing of personal data,

HAVING REGARD to Section 26 of Act no. 14 of 3 February 2003, setting out provisions to ensure compliance with obligations related to Italy's membership in the European Communities (Community Act of 2002),

HAVING REGARD to Act no. 675 of 31 December 1996 as subsequently amended,

HAVING REGARD to Act no. 676 of 31 December 1996, enabling Government to pass legislation concerning protection of individual and other entities with regard to the processing of personal data,

HAVING REGARD to 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,

HAVING REGARD to Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002, on the processing of personal data and the protection of private life in the electronic communications sector,

HAVING REGARD to the preliminary resolution adopted by the Council of Ministers at its meeting of 9 May 2003,

HAVING HEARD the Garante per la protezione dei dati personali,

HAVING ACQUIRED the opinion by the competent Parliamentary committees at the Chamber of Deputies and the Senate of the Republic,

HAVING REGARD to the Council of Ministers' resolution adopted at the meeting of 27 June 2003,

ACTING ON THE PROPOSAL put forward by the Prime Minister, the Minister for Public Administration and the Minister for Community Policies, in agreement with the Ministers of Justice, of Economy and Finance, of Foreign Affairs and Communications,

ISSUES

the following legislative decree:

PART 1 – GENERAL PROVISIONS

TITLE I – GENERAL PRINCIPLES

Section 1

(Right to the Protection of Personal Data)

1. Everyone has the right to protection of the personal data concerning them. [Repealed][1].

Section 2

(Purposes)

1. This consolidated statute, hereinafter referred to as "Code", shall ensure that personal data are processed by respecting data subjects' rights, fundamental freedoms and dignity, particularly with regard to confidentiality, personal identity and the right to personal data protection.

2. The processing of personal data shall be regulated by affording a high level of protection for the rights and freedoms referred to in paragraph 1 in compliance with the principles of simplification, harmonisation and effectiveness of the mechanisms by which data subjects can exercise such rights and data controllers can fulfil the relevant obligations.

Section 3

(Data Minimisation Principle)

1. Information systems and software shall be configured by minimising the use of personal data and identification data, in such a way as to rule out their processing if the purposes sought in the individual cases can be achieved by using either anonymous data or suitable arrangements to allow identifying data subjects only in cases of necessity, respectively.

Section 4

(Definitions)

1. For the purposes of this Code,

[1] The final sentence added by section 4(9) of Act no. 15 dated 4 March 2009 was subsequently repealed by section 14(1)a. of Act no. 183/2010.

a) ‘processing’ shall mean any operation, or set of operations, carried out with or without the help of electronic or automated means, concerning the collection, recording, organisation, keeping, interrogation, elaboration, modification, selection, retrieval, comparison, utilization, interconnection, blocking, communication, dissemination, erasure and destruction of data, whether the latter are contained or not in a data bank;

b) ‘personal data’ shall mean any information relating to natural persons that are or can be identified, even indirectly, by reference to any other information including a personal identification number;[2]

c) ‘identification data’ shall mean personal data allowing a data subject to be directly identified;

d) ‘sensitive data’ shall mean personal data allowing the disclosure of racial or ethnic origin, religious, philosophical or other beliefs, political opinions, membership of parties, trade unions, associations or organizations of a religious, philosophical, political or trade-unionist character, as well as personal data disclosing health and sex life;

e) ‘judicial data’ shall mean personal data disclosing the measures referred to in Section 3(1), letters a) to o) and r) to u), of Presidential Decree no. 313 of 14 November 2002 concerning the criminal record office, the register of offence-related administrative sanctions and the relevant current charges, or the status of being either defendant or the subject of investigations pursuant to Sections 60 and 61 of the Criminal Procedure Code;

f) ‘data controller’ shall mean any natural or legal person, public administration, body, association or other entity that is competent, also jointly with another data controller, to determine purposes and methods of the processing of personal data and the relevant means, including security matters;

g) ‘data processor’ shall mean any natural or legal person, public administration, body, association or other agency that processes personal data on the controller’s behalf;

h) ‘persons in charge of the processing” shall mean the natural persons that have been authorised by the data controller or processor to carry out processing operations;

i) ‘data subject’ shall mean any natural person that is the subject of the personal data;[3]

l) ‘communication’ shall mean disclosing personal data to one or more identified entities other than the data subject, the data controller’s representative in the State’s territory, the data processor and persons in charge of the processing in any form whatsoever, including by making available or interrogating such data;

m) ‘dissemination’ shall mean disclosing personal data to unidentified entities, in any form whatsoever, including by making available or interrogating such data;

n) ‘anonymous data’ shall mean any data that either in origin or on account of its having been processed cannot be associated with any identified or identifiable data subject;

---

[2] As amended by Section 40(2)a. of decree no. 201 dated 6 December 2011 subsequently converted, with amendments, into Act no. 214 dated 22 December 2011.

[3] As amended by Section 40(2)b. of decree no. 201 dated 6 December 2011 subsequently converted, with amendments, into Act no. 214 dated 22 December 2011

o) ‘blocking’ shall mean keeping personal data by temporarily suspending any other processing operation;

p) ‘data bank’ shall mean any organised set of personal data, divided into one or more units located in one or more places;

q) ‘Garante’ shall mean the authority referred to in Section 153 as set up under Act no. 675 of 31 December 1996.

2. Furthermore, for the purposes of this Code,

a) ‘electronic communication’ shall mean any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable or identified subscriber or user receiving the information;

b) ‘call’ means a connection established by means of a publicly available telephone service allowing two-way communication in real time;

c) ‘electronic communications network’ shall mean transmission systems and switching or routing equipment and other resources which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, networks used for radio and television broadcasting, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, and cable television networks, irrespective of the type of information conveyed;

d) ‘public communications network shall mean an electronic communications network used wholly or mainly for the provision of publicly available electronic communications services;

e) ‘electronic communications service’ shall mean a service which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, to the extent that this is provided for in Article 2, letter c) of Directive 2202/21/EC of the European Parliament and of the Council of 7 March 2002;

f) ‘subscriber’ shall mean any natural or legal person, body or association who or which is party to a contract with the provider of publicly available electronic communications services for the supply of such services, or is anyhow the recipient of such services by means of pre-paid cards;

g) ‘user’ shall mean a natural person using a publicly available electronic communications service for private or business purposes, without necessarily being a subscriber to such service;

h) ‘traffic data’ shall mean any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof;

i) ‘location data’ shall mean any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service;

l) ‘value added service’ shall mean any service which requires the processing of traffic data or location data other than traffic data beyond what is necessary for the transmission of a communication or the billing thereof;

m) ‘electronic mail’ shall mean any text, voice, sound or image message sent over a public communications network, which can be stored in the network or in the recipient’s terminal equipment until it is collected by the recipient.

3. And for the purposes of this Code,

a) ‘minimum measures’ shall mean the technical, informational, organizational, logistics and procedural security measures affording the minimum level of protection which is required by having regard to the risks mentioned in Section 31;

b) ‘electronic means’ shall mean computers, computer software and any electronic and/or automated device used for performing the processing;

c) “computerised authentication” shall mean a set of electronic tools and procedures to verify identity also indirectly,

d) “authentication credentials” shall mean the data and devices in the possession of a person, whether known by or uniquely related to the latter, that are used for computer authentication,

e) “password” shall mean the component of an authentication credential associated with and known to a person, consisting of a sequence of characters or other data in electronic format,

f) “authorisation profile” shall mean the information uniquely associated with a person that allows determining the data that may be accessed by said person as well as the processing operations said person may perform,

g) “authorisation system” shall mean the tools and procedures enabling access to the data and the relevant processing mechanisms as a function of the requesting party’s authorisation profile.

4. For the purposes of this Code,

a) "historical purposes" shall mean purposes related to studies, investigations, research and documentation concerning characters, events and situations of the past;

b) "statistical purposes" shall mean purposes related to statistical investigations or the production of statistical results, also by means of statistical information systems;

c) "scientific purposes" shall mean purposes related to studies and systematic investigations that are aimed at developing scientific knowledge in a given sector.

Section 5

(Subject-Matter and Scope of Application)

1. This Code shall apply to the processing of personal data, including data held abroad, where the processing is performed by any entity established either in the State's territory or in a place that is under the State's sovereignty.

2. This Code shall also apply to the processing of personal data that is performed by an entity established in the territory of a country outside the European Union, where said entity makes use in connection with the processing of equipment, whether electronic or otherwise, situated in the State's territory, unless such equipment is used only for purposes of transit through the territory of the European Union. If this Code applies, the data controller shall designate a representative established in the State's territory with a view to implementing the provisions concerning processing of personal data.

3. This Code shall only apply to the processing of personal data carried out by natural persons for exclusively personal purposes if the data are intended for systematic communication or dissemination. The provisions concerning liability and security referred to in Sections 15 and 31 shall apply in any case.

3-bis. [Repealed by Section 40(2)c. of decree no. 201 dated 6 December 2011 subsequently converted, with amendments, into Act no. 214 dated 22 December 2011].

Section 6

(Regulations Applying to Processing Operations)

1. The provisions contained in this Part shall apply to any processing operations except as specified in connection with some processing operations by the provisions contained in Part II that amend and/or supplement those laid down herein.

TITLE II – DATA SUBJECT'S RIGHTS

Section 7

(Right to Access Personal Data and Other Rights)

1. A data subject shall have the right to obtain confirmation as to whether or not personal data concerning him exist, regardless of their being already recorded, and communication of such data in intelligible form.

2. A data subject shall have the right to be informed

a) of the source of the personal data;

b) of the purposes and methods of the processing;

c) of the logic applied to the processing, if the latter is carried out with the help of electronic means;

d) of the identification data concerning data controller, data processors and the representative designated as per Section 5(2);

e) of the entities or categories of entity to whom or which the personal data may be communicated and who or which may get to know said data in their capacity as designated representative(s) in the State's territory, data processor(s) or person(s) in charge of the processing.

3. A data subject shall have the right to obtain

a) updating, rectification or, where interested therein, integration of the data;

b) erasure, anonymization or blocking of data that have been processed unlawfully, including data whose retention is unnecessary for the purposes for which they have been collected or subsequently processed;

c) certification to the effect that the operations as per letters a) and b) have been notified, as also related to their contents, to the entities to whom or which the data were communicated or disseminated, unless this requirement proves impossible or involves a manifestly disproportionate effort compared with the right that is to be protected.

4. A data subject shall have the right to object, in whole or in part,

a) on legitimate grounds, to the processing of personal data concerning him/her, even though they are relevant to the purpose of the collection;

b) to the processing of personal data concerning him/her, where it is carried out for the purpose of sending advertising materials or direct selling or else for the performance of market or commercial communication surveys.

Section 8

(Exercise of Rights)

1. The rights referred to in Section 7 may be exercised by making a request to the data controller or processor without formalities, also by the agency of a person in charge of the processing. A suitable response shall be provided to said request without delay.

2. The rights referred to in Section 7 may not be exercised by making a request to the data controller or processor, or else by lodging a complaint in pursuance of Section 145, if the personal data are processed:

a) pursuant to the provisions of decree-law no. 143 of 3 May 1991, as converted, with amendments, into Act no. 197 of 5 July 1991 and subsequently amended, concerning money laundering;

b) pursuant to the provisions of decree-law no. 419 of 31 December 1991, as converted, with amendments, into Act no. 172 of 18 February 1992 and subsequently amended, concerning support for victims of extortion;

c) by parliamentary Inquiry Committees set up as per Article 82 of the Constitution;

d) by a public body other than a profit-seeking public body, where this is expressly required by a law for purposes exclusively related to currency and financial policy, the system of payments, control of brokers and credit and financial markets and protection of their stability;

e) in pursuance of Section 24(1), letter f), as regards the period during which performance of the investigations by defence counsel or establishment of the legal claim might be actually and concretely prejudiced;

f) by providers of publicly available electronic communications services in respect of incoming phone calls, unless this may be actually and concretely prejudicial to performance of the investigations by defence counsel as per Act no. 397 of 7 December 2000;

g) for reasons of justice by judicial authorities at all levels and of all instances as well as by the Higher Council of the Judiciary or other self-regulatory bodies, or else by the Ministry of Justice;

h) in pursuance of Section 53, without prejudice to Act no. 121 of 1 April 1981.

3. In the cases referred to in paragraph 2, letters a), b), d), e) and f), the Garante, also following a report submitted by the data subject, shall act as per Sections 157, 158 and 159; in the cases referred to in letters c), g) and h) of said paragraph, the Garante shall act as per Section 160.

4. Exercise of the rights referred to in Section 7 may be permitted with regard to data of non-objective character on condition that it does not concern rectification of or additions to personal evaluation data in connection with judgments, opinions and other types of subjective assessment, or else the specification of policies to be implemented or decision-making activities by the data controller.

Section 9

(Mechanisms to Exercise Rights)

1. The request addressed to the data controller or processor may also be conveyed by means of a registered letter, facsimile or e-mail. The Garante may specify other suitable arrangements with regard to new technological solutions. If the request is related to exercise of the rights referred to in Section 7(1) and (2), it may also be made verbally; in this case, it will be written down in summary fashion by either a person in charge of the processing or the data processor.

2. The data subject may grant, in writing, power of attorney or representation to natural persons, bodies, associations or organisations in connection with exercise of the rights as per Section 7. The data subject may also be assisted by a person of his/her choice.

3. The rights as per Section 7, where related to the personal data concerning a deceased, may be exercised by any entity that is interested therein or else acts to protect a data subject or for family-related reasons deserving protection.

4. The data subject's identity shall be verified on the basis of suitable information, also by means of available records or documents or by producing or attaching a copy of an identity document. The person acting on instructions from the data subject must produce or attach a copy of either the proxy or the letter of attorney, which shall have been undersigned by the data subject in the presence of a person in charge thereof or else shall bear the data subject's signature and be produced jointly with a copy of an ID document from the data subject, which shall not have to be certified true pursuant to law.[4]

5. The request referred to in Section 7(1) and (2) may be worded freely without any constraints and may be renewed at intervals of not less than ninety days, unless there are well-grounded reasons.

Section 10

(Response to Data Subjects)

1. With a view to effectively exercising the rights referred to in Section 7, data controllers shall take suitable measures in order to, in particular,

a) facilitate access to personal data by the data subjects, even by means of ad hoc software allowing accurate retrieval of the data concerning individual identified or identifiable data subjects;
b) simplify the arrangements and reduce the delay for the responses, also with regard to public relations departments or offices.

2. The data processor or the person(s) in charge of the processing shall be responsible for retrieval of the data, which may be communicated to the requesting party also verbally, or else displayed by electronic means - on condition that the data are easily intelligible in such cases also in the light of the nature and amount of the information. The data shall be reproduced on paper or magnetic media, or else transmitted via electronic networks, whenever this is requested.

3. The response provided to the data subject shall include all the personal data concerning him/her that are processed by the data controller, unless the request concerns either a specific processing operation or specific personal data or categories of personal data. If the request is made to a health care professional or health care body, Section 84(1) shall apply.

4. If data retrieval is especially difficult, the response to the data subject's request may also consist in producing or delivering copy of records and documents containing the personal data at stake.

[4] As amended by Section 40(2)d. of decree no. 201 dated 6 December 2011 subsequently converted, with amendments, into Act no. 214 dated 22 December 2011; the amendment repealed the final period in this paragraph, which read as follows: "If the data subject is a legal person, a body or association, the relevant request shall be made by the natural person that is legally authorized thereto based on the relevant regulations or articles of association."

5. The right to obtain communication of the data in intelligible form does not apply to personal data concerning third parties, unless breaking down the processed data or eliminating certain items from the latter prevents the data subject's personal data from being understandable.

6. Data are communicated in intelligible form also by using legible handwriting. If codes or abbreviations are communicated, the criteria for understanding the relevant meanings shall be made available also by the agency of the persons in charge of the processing.

7. Where it is not confirmed that personal data concerning the data subject exist, further to a request as per Section 7(1) and (2), letters a), b) and c), the data subject may be charged a fee which shall not be in excess of the costs actually incurred for the inquiries made in the specific case.

8. The fee referred to in paragraph 7 may not be in excess of the amount specified by the Garante in a generally applicable provision, which may also refer to a lump sum to be paid in case the data are processed by electronic means and the response is provided verbally. Through said instrument the Garante may also provide that the fee may be charged if the personal data are contained on special media whose reproduction is specifically requested, or else if a considerable effort is required by one or more data controllers on account of the complexity and/or amount of the requests and existence of data concerning the data subject can be confirmed.

9. The fee referred to in paragraphs 7 and 8 may also be paid by bank or postal draft, or else by debit or credit card, if possible upon receiving the relevant response and anyhow within fifteen days of said response.

TITLE III – GENERAL DATA PROCESSING RULES

CHAPTER I – RULES APPLYING TO ALL PROCESSING OPERATIONS

Section 11

(Processing Arrangements and Data Quality)

1. Personal data undergoing processing shall be:

a) processed lawfully and fairly;

b) collected and recorded for specific, explicit and legitimate purposes and used in further processing operations in a way that is not inconsistent with said purposes;

c) accurate and, when necessary, kept up to date;

d) relevant, complete and not excessive in relation to the purposes for which they are collected or subsequently processed;

e) kept in a form which permits identification of the data subject for no longer than is necessary for the purposes for which the data were collected or subsequently processed.

2. Any personal data that is processed in breach of the relevant provisions concerning the processing of personal data may not be used.

Section 12

(Codes of Conduct and Professional Practice)

1. The Garante shall encourage, within the framework of the categories concerned and in conformity with the principle of representation, by having regard to the guidelines set out in Council of Europe recommendations on the processing of personal data, the drawing up of codes of conduct and professional practice for specific sectors, verify their compliance with laws and regulations by also taking account of the considerations made by the entities concerned, and contribute to adoption of and compliance with such codes.

2. The Garante shall be responsible for having the codes published in the Official Journal of the Italian Republic; the codes shall be included into Annex A) to this Code based on a decree by the Minister of Justice.

3. Compliance with the provisions included in the codes referred to in paragraph 1 shall be a prerequisite for the processing of personal data by public and private entities to be lawful.

4. The provisions of this Section shall also apply to the code of conduct on the processing of data for journalistic purposes as adopted further to the encouragement provided by the Garante in pursuance of paragraph 1 and Section 139.

Section 13

(Information to Data Subjects)

1. The data subject as well as any entity from whom or which personal data are collected shall be preliminarily informed, either orally or in writing, as to:

a) the purposes and modalities of the processing for which the data are intended;

b) the obligatory or voluntary nature of providing the requested data;

c) the consequences if (s)he fails to reply;

d) the entities or categories of entity to whom or which the data may be communicated, or who/which may get to know the data in their capacity as data processors or persons in charge of the processing, and the scope of dissemination of said data;

e) the rights as per Section 7;

f) the identification data concerning the data controller and, where designated, the data controller's representative in the State's territory pursuant to Section 5 and the data processor. If several data processors have been designated by the data controller, at least one among them shall be referred to and either the site on the communications network or the mechanisms for easily accessing the updated list of data processors shall be specified. If a data processor has been designated to provide responses to data subjects in case the rights as per Section 7 are exercised, such data processor shall be referred to.

2. The information as per paragraph 1 shall also contain the items referred to in specific provisions of this Code and may fail to include certain items if the latter are already known to the entity providing the data or their knowledge may concretely impair supervisory or control activities carried out by public bodies for purposes related to defence or State security, or else for the prevention, suppression or detection of offences.

3. The Garante may issue a provision to set out simplified information arrangements as regards, in particular, telephone services providing assistance and information to the public.

4. Whenever the personal data are not collected from the data subject, the information as per paragraph 1, also including the categories of processed data, shall be provided to the data subject at the time of recording such data or, if their communication is envisaged, no later than when the data are first communicated.

5. Paragraph 4 shall not apply

a) if the data are processed in compliance with an obligation imposed by a law, regulations or Community legislation;

b) if the data are processed either for carrying out the investigations by defence counsel as per Act no. 397 of 07.12.2000 or to establish or defend a legal claim, provided that the data are processed exclusively for said purposes and for no longer than is necessary therefor;

c) if the provision of information to the data subject involves an effort that is declared by the Garante to be manifestly disproportionate compared with the right to be protected, in which case the Garante shall lay down suitable measures, if any, or if it proves impossible in the opinion of the Garante.

5-bis. The information as per paragraph 1 shall not be necessary in case CVs are received that are sent voluntarily by the relevant data subjects with a view to recruitment for job positions. When first contacting a data subject that has sent his/her CV, the data controller shall be required to provide such data subject, also verbally, with a short information notice that shall include at least the items mentioned in paragraph 1, letters a., d., and f. . [Paragraph added by Section 6(2)a, item 2. of decree no. 70 dated 13 May 2011 as converted, with amendments, into Act no. 106 dated 12 July 2011]

Section 14

(Profiling of Data Subjects and Their Personality)

1. No judicial or administrative act or measure involving the assessment of a person's conduct may be based solely on the automated processing of personal data aimed at defining the data subject's profile or personality.

2. The data subject may challenge any other decision that is based on the processing referred to in paragraph 1, pursuant to Section 7(4), letter a), unless such decision has been taken for the conclusion or performance of a contract, further to a proposal made by the data subject or on the basis of adequate safeguards laid down either by this Code or in a provision issued by the Garante in pursuance of Section 17.

Section 15

(Damage Caused on Account of the Processing)

1. Whoever causes damage to another as a consequence of the processing of personal data shall be liable to pay damages pursuant to Section 2050 of the Civil Code.

2. Compensation for non-pecuniary damage shall be also due upon infringement of Section 11.

Section 16

(Termination of Processing Operations)

1. Should data processing be terminated, for whatever reason, the data shall be

a) destroyed;

b) assigned to another data controller, provided they are intended for processing under terms that are compatible with the purposes for which the data have been collected;

c) kept for exclusively personal purposes, without being intended for systematic communication or dissemination;

d) kept or assigned to another controller for historical, scientific or statistical purposes, in compliance with laws, regulations, Community legislation and the codes of conduct and professional practice adopted in pursuance of Section 12.

2. Assignment of data in breach either of paragraph 1, letter b), or of other relevant provisions applying to the processing of personal data shall be void.

Section 17

(Processing Operations Carrying Specific Risks)

1. Processing of data other than sensitive and judicial data shall be allowed in accordance with such measures and precautions as are laid down to safeguard data subjects, if the processing is likely to present specific risks to data subjects' fundamental rights and freedoms and dignity on account of the nature of the data, the arrangements applying to the processing or the effects the latter may produce.

2. The measures and precautions referred to in paragraph 1 shall be laid down by the Garante on the basis of the principles set out in this Code within the framework of a check to be performed prior to start of the processing as also related to specific categories of data controller or processing, following the request, if any, submitted by the data controller.

CHAPTER II – ADDITIONAL RULES APPLYING TO PUBLIC BODIES

Section 18

(Principles Applying to All Processing Operations Performed by Public Bodies)

1. The provisions of this Chapter shall apply to all public bodies except for profit-seeking public bodies.

2. Public bodies shall only be permitted to process personal data in order to discharge their institutional tasks.

3. In processing the data, public bodies shall abide by the prerequisites and limitations set out in this Code, by having also regard to the different features of the data, as well as in laws and regulations.

4. Subject to the provisions of Part II as applying to health care professionals and public health care organisations, public bodies shall not be required to obtain the data subject's consent.

5. The provisions laid down in Section 25 as for communication and dissemination shall apply.

Section 19

(Principles Applying to the Processing of Data Other Than Sensitive and Judicial Data)

1. Public bodies may process data other than sensitive and judicial data also in the absence of laws or regulations providing expressly for such processing, subject to Section 18(2).

2. Communication by a public body to other public bodies shall be permitted if it is envisaged by laws or regulations. Failing such laws or regulations, communication shall be permitted if it is

necessary in order to discharge institutional tasks and may be started upon expiry of the term referred to in Section 39(2) if it has not been provided otherwise as specified therein.

3. Communication by a public body to private entities or profit-seeking public bodies as well as dissemination by a public body shall only be permitted if they are provided for by laws or regulations.

3-bis. The information concerning performance of the tasks committed to any person that is in charge of public functions including the respective evaluation shall be made available by the public employer. Except where provided for by law, no information may be disclosed concerning nature of the medical conditions and/or personal or family circumstances resulting into a person's absence from the workplace or else the elements making up the evaluation or any information on the employment relationship between the aforementioned public employee and the public employer if they are suitable for disclosing any items of information referred to in section 4(1)d. hereof.[5]

Section 20

(Principles Applying to the Processing of Sensitive Data)

1. Processing of sensitive data by public bodies shall only be allowed where it is expressly authorised by a law specifying the categories of data that may be processed and the categories of operation that may be performed as well as the substantial public interest pursued.

2. Whenever the substantial public interest is specified by a law in which no reference is made to the categories of sensitive data and the operations that may be carried out, processing shall only be allowed with regard to the categories of data and operation that have been specified and made public by the entities processing such data, having regard to the specific purposes sought in the individual cases and in compliance with the principles referred to in Section 22, via regulations or regulations-like instruments that shall be adopted pursuant to the opinion rendered by the Garante under Section 154(1), letter g), also on the basis of draft models.

3. If the processing is not provided for expressly by a law, public bodies may request the Garante to determine the activities that pursue a substantial public interest among those they are required to discharge under the law. Processing of sensitive data shall be authorised in pursuance of Section 26(2) with regard to said activities, however it shall only be allowed if the public bodies also specify and make public the categories of data and operation in the manner described in paragraph 2.

4. The specification of the categories of data and operation referred to in paragraphs 2 and 3 shall be updated and supplemented regularly.

[5] This paragraph was added by section 14(1)b. of Act no. 183/2010.

Section 21

(Principles Applying to the Processing of Judicial Data)

1. Processing of judicial data by public bodies shall only be permitted where expressly authorized by a law or an order of the Garante specifying the purposes in the substantial public interest underlying such processing, the categories of data to be processed and the operations that may be performed.

2. Section 20(2) and (4) shall also apply to processing of judicial data.

Section 22

(Principles Applying to the Processing of Sensitive Data as well as to Judicial Data)

1. Public bodies shall process sensitive and judicial data in accordance with arrangements aimed at preventing breaches of data subjects' rights, fundamental freedoms and dignity.

2. When informing data subjects as per Section 13, public bodies shall expressly refer to the provisions setting out the relevant obligations or tasks, on which the processing of sensitive and judicial data is grounded.

3. Public bodies may process exclusively such sensitive and judicial data as are indispensable for them to discharge institutional tasks that cannot be performed, on a case by case basis, by processing anonymous data or else personal data of a different nature

4. Sensitive and judicial data shall be collected, as a rule, from the data subject.

5. In pursuance of Section 11(1), letters c), d) and e), public bodies shall regularly check that sensitive and judicial data are accurate and updated, and that they are relevant, complete, not excessive and indispensable with regard to the purposes sought in the individual cases - including the data provided on the data subject's initiative. With a view to ensuring that sensitive and judicial data are indispensable in respect of their obligations and tasks, public bodies shall specifically consider the relationship between data and tasks to be fulfilled. No data that is found to be excessive, irrelevant or unnecessary, also as a result of the above checks, may be used, except for the purpose of keeping - pursuant to law - the record or document containing said data. Special care shall be taken in checking that sensitive and judicial data relating to entities other than those which are directly concerned by the service provided or the tasks to be fulfilled are indispensable.

6. Sensitive or judicial data that are contained in lists, registers or data banks kept with electronic means shall be processed by using encryption techniques, identification codes or any other system such as to make the data temporarily unintelligible also to the entities authorised to access them and allow identification of the data subject only in case of necessity, by having regard to amount and nature of the processed data.

7. Data disclosing health and sex life shall be kept separate from any other personal data that is processed for purposes for which they are not required. Said data shall be processed in accordance with the provisions laid down in paragraph 6 also if they are contained in lists, registers or data banks that are kept without the help of electronic means.

8. Data disclosing health may not be disseminated.

9. As for the sensitive and judicial data that are necessary pursuant to paragraph 3, public bodies shall be authorized to carry out exclusively such processing operations as are indispensable to achieve the purposes for which the processing is authorized, also if the data are collected in connection with discharging supervisory, control or inspection tasks.

10. Sensitive and judicial data may not be processed within the framework of psychological and behavioural tests aimed at defining the data subject's profile or personality. Sensitive and judicial data may only be matched as well as processed in pursuance of Section 14 if the grounds therefor are preliminarily reported in writing.

11. In any case, the operations and processing referred to in paragraph 10, if performed by using data banks from different data controllers, as well as the dissemination of judicial and sensitive data shall only be allowed if they are expressly provided for by law.

12. This Section shall set out principles that are applicable to the processing operations provided for by the Office of the President of the Republic, the Chamber of Deputies, the Senate of the Republic and the Constitutional Court, in pursuance of their respective regulations.

CHAPTER III – ADDITIONAL RULES APPLYING TO PRIVATE BODIES AND PROFIT-SEEKING PUBLIC BODIES

Section 23

(Consent)

1. Processing of personal data by private entities or profit-seeking public bodies shall only be allowed if the data subject gives his/her express consent

2. The data subject's consent may refer either to the processing as a whole or to one or more of the operations thereof.

3. The data subject's consent shall only be deemed to be effective if it is given freely and specifically with regard to a clearly identified processing operation, if it is documented in writing, and if the data subject has been provided with the information referred to in Section 13.

4. Consent shall be given in writing if the processing concerns sensitive data.

Section 24

(Cases in Which No Consent Is Required for Processing Data)

1. Consent shall not be required in the cases referred to in Part II as well as if the processing

a) is necessary to comply with an obligation imposed by a law, regulations or Community legislation;

b) is necessary for the performance of obligations resulting from a contract to which the data subject is a party, or else in order to comply with specific requests made by the data subject prior to entering into a contract;

c) concerns data taken from public registers, lists, documents or records that are publicly available, without prejudice to the limitations and modalities laid down by laws, regulations and Community legislation with regard to their disclosure and publicity;

d) concerns data relating to economic activities that are processed in compliance with the legislation in force as applying to business and industrial secrecy;

e) is necessary to safeguard life or bodily integrity of a third party. If this purpose concerns the data subject and the latter cannot give his/her consent because (s)he is physically unable to do so, legally incapable or unable to distinguish right and wrong, the consent shall be given by the entity legally representing the data subject, or else by a next of kin, a family member, a person cohabiting with the data subject or, failing these, the manager of the institution where the data subject is hosted. Section 82(2) shall apply;

f) is necessary for carrying out the investigations by defence counsel referred to in Act no. 397 of 07.12.2000, or else to establish or defend a legal claim, provided that the data are processed exclusively for said purposes and for no longer than is necessary therefor by complying with the legislation in force concerning business and industrial secrecy, dissemination of the data being ruled out;

g) is necessary to pursue a legitimate interest of either the data controller or a third party recipient in the cases specified by the Garante on the basis of the principles set out under the law, unless said interest is overridden by the data subject's rights and fundamental freedoms, dignity or legitimate interests, dissemination of the data being ruled out; [Amended by Section 6(2)a, item 3. of decree no. 70 dated 13 May 2011 as converted, with amendments, into Act no. 106 dated 12 July 2011]

h) except for external communication and dissemination, is carried out by no-profit associations, bodies or organisations, recognised or not, with regard either to entities having regular contacts with them or to members in order to achieve specific, lawful purposes as set out in the relevant memorandums, articles of association or collective agreements, whereby the mechanisms of utilisation are laid down expressly in a resolution that is notified to data subjects with the information notice provided for by Section 13,

i) is necessary exclusively for scientific and statistical purposes in compliance with the respective codes of professional practice referred to in Annex A), or else exclusively for historical purposes in connection either with private archives that have been declared to be of considerable historical interest pursuant to Section 6(2) of legislative decree no. 499 of 29 October 1999, adopting the consolidated statute on cultural and environmental heritage, or with other private archives pursuant to the provisions made in the relevant codes;

i-bis) concerns information contained in the CVs as per Section 13(5-bis); [Added by Section 6(2)a, item 3. of decree no. 70 dated 13 May 2011 as converted, with amendments, into Act no. 106 dated 12 July 2011]

i-ter) except for dissemination and subject to Section 130 hereof, concerns communication of data between companies, bodies and/or associations and parent, subsidiary and/or related companies pursuant to Section 2359 of the Civil Code, or between the former and jointly controlled companies, or between consortiums, corporate networks and/or corporate joint ventures and the respective members, for the administrative and accounting purposes specified in Section 34(1-ter) hereof, providing such purposes are expressly referred to in a decision that shall be disclosed to data subjects jointly with the information notice referred to in Section 13 hereof. [Added by Section 6(2)a, item 3. of decree no. 70 dated 13 May 2011 as converted, with amendments, into Act no. 106 dated 12 July 2011]

Section 25

(Bans on Communication and Dissemination)

1. Communication and dissemination shall be prohibited if an order to this effect has been issued by either the Garante or judicial authorities, as well as

a) with regard to personal data that must be erased by order, or else upon expiry of the term referred to in Section 11(1), letter e),

b) for purposes other than those specified in the notification, whenever the latter is to be submitted.

2. This shall be without prejudice to communication and dissemination of the data as requested, pursuant to law, by police, judicial authorities, intelligence and security agencies and other public bodies according to Section 58(2), for purposes of defence or relating to State security, or for the prevention, detection or suppression of offences.

Section 26

(Safeguards Applying to Sensitive Data)

1. Sensitive data may only be processed with the data subject's written consent and the Garante's prior authorisation, by complying with the prerequisites and limitations set out in this Code as well as in laws and regulations.

2. The Garante shall communicate its decision concerning the request for authorisation within forty-five days; failing a communication at the expiry of said term, the request shall be regarded as dismissed. Along with the authorisation or thereafter, based also on verification, the Garante may provide for measures and precautions in order to safeguard the data subject, which the data controller shall be bound to apply.

3. Paragraph 1 shall not apply to processing

a) of the data concerning members of religious denominations and entities having regular contact with said denominations for exclusively religious purposes, on condition that the data are processed by the relevant organs or bodies recognised under civil law and are not communicated or

disseminated outside said denominations. The latter shall lay down suitable safeguards with regard to the processing operations performed by complying with the relevant principles as set out in an authorisation by the Garante;

b) of the data concerning affiliation of trade unions and/or trade associations or organisations to other trade unions and/or trade associations, organisations or confederations;

b-bis) of the data contained in CVs under the terms set forth in Section 13(5-bis) hereof. [Added by Section 6(2)a, item 4. of decree no. 70 dated 13 May 2011 as converted, with amendments, into Act no. 106 dated 12 July 2011]

4. Sensitive data may also be processed without consent, subject to the Garante's authorisation,

a) if the processing is carried out for specific, lawful purposes as set out in the relevant memorandums, articles of association or collective agreements by not-for-profit associations, bodies or organisations, whether recognised or not, of political, philosophical, religious or trade-unionist nature, including political parties and movements, with regard to personal data concerning members and/or entities having regular contacts with said associations, bodies or organisations in connection with the aforementioned purposes, provided that the data are not communicated or disclosed outside and the bodies, associations or organisations lay down suitable safeguards in respect of the processing operations performed by expressly setting out the arrangements for using the data through a resolution that shall be made known to data subjects at the time of providing the information under Section 13;

b) if the processing is necessary to protect a third party's life or bodily integrity. If this purpose concerns the data subject and the latter cannot give his/her consent because (s)he is physically unable to do so, legally incapable or unable to distinguish right and wrong, the consent shall be given by the entity legally representing the data subject, or else by a next of kin, a family member, a person cohabiting with the data subject or, failing these, the manager of the institution where the data subject is hosted. Section 82(2) shall apply;

c) if the processing is necessary for carrying out the investigations by defence counsel referred to in Act no. 397 of 07.12.2000, or else to establish or defend a legal claim, provided that the data are processed exclusively for said purposes and for no longer than is necessary therefor. Said claim must not be overridden by the data subject's claim, or else must consist in a personal right or another fundamental, inviolable right or freedom, if the data can disclose health and sex life;

d) if the processing is necessary to comply with specific obligations and/or tasks laid down by laws, regulations or Community legislation in the employment context, also with regard to occupational and population hygiene and safety and to social security and assistance purposes, to the extent that it is provided for in the authorisation and subject to the requirements of the code of conduct and professional practice referred to in Section 111.

5. Data disclosing health may not be disseminated.

Section 27

(Safeguards Applying to Judicial Data)

1. Processing of judicial data by private entities and profit-seeking public bodies shall be permitted only where expressly authorized by a law or an order by the Garante specifying the reasons in the substantial public interest underlying such processing, the categories of processed data and the operations that may be performed.

TITLE IV – ENTITIES PERFORMING PROCESSING OPERATIONS

Section 28

(Data Controller)

1. Whenever processing operations are carried out by a legal person, a public administrative agency or any other body, association or organisation, the data controller shall be either the entity as a whole or the department or peripheral unit having fully autonomous decision-making powers in respect of purposes and mechanisms of said processing operations as also related to security matters.

Section 29

(Data Processor)

1. The data processor may be designated by the data controller on an optional basis.

2. Where designated, the data processor shall be selected among entities that can appropriately ensure, on account of their experience, capabilities and reliability, thorough compliance with the provisions in force applying to processing as also related to security matters.

3. If necessary on account of organizational requirements, several entities may be designated as data processors also by subdividing the relevant tasks.

4. The tasks committed to the data processor shall be detailed in writing by the data controller.

5. The data processor shall abide by the instructions given by the data controller in carrying out the processing. The data controller shall supervise over thorough compliance with both said instructions and the provisions referred to in paragraph 2, also by means of regular controls.

Section 30

(Persons in Charge of the Processing)

1. Processing operations may only be performed by persons in charge of the processing that act under the direct authority of either the data controller or the data processor by complying with the instructions received.

2. The aforementioned persons shall be nominated in writing by specifically referring to the scope of the processing operations that are permitted. This requirement shall be also fulfilled if a natural person is entrusted with the task of directing a department, on a documentary basis, whereby the scope of the processing operations that may be performed by the staff working in said department has been specified in writing.

TITLE V – DATA AND SYSTEM SECURITY

CHAPTER I – SECURITY MEASURES

Section 31

(Security Requirements)

1. Personal data undergoing processing shall be kept and controlled, also in consideration of technological innovations, of their nature and the specific features of the processing, in such a way as to minimise, by means of suitable preventative security measures, the risk of their destruction or loss, whether by accident or not, of unauthorized access to the data or of processing operations that are either unlawful or inconsistent with the purposes for which the data have been collected.

Section 32

(Specific Categories of Data Controller)

1. The provider of a publicly available electronic communications service shall take suitable technical and organisational measures under Section 31 that are adequate in the light of the existing risk, in order to safeguard security of its services and integrity of traffic data, location data and electronic communications against any form of unauthorised utilisation or access.

2. Whenever security of service or personal data makes it necessary to also take measures applying to the network, the provider of a publicly available electronic communications service shall take those measures jointly with the provider of the public communications network. Failing an agreement between said providers, the dispute shall be settled, at the instance of either provider, by the Authority for Communications Safeguards in pursuance of the arrangements set out in the legislation in force.

3. In case of a particular risk of a breach of network security, the provider of a publicly available electronic communications service shall inform subscribers and, if possible, users concerning said risk and, when the risk lies outside the scope of the measures to be taken by said provider pursuant to paragraphs 1 and 2, of all the possible remedies including an indication of the likely costs involved. This information shall be also provided to the Garante and the Authority for Communications Safeguards.

CHAPTER II – MINIMUM SECURITY MEASURES

Section 33

(Minimum Security Measures)

1. Within the framework of the more general security requirements referred to in Section 31, or else provided for by specific regulations, data controllers shall be required in any case to adopt the minimum security measures pursuant either to this Chapter or to Section 58(3) in order to ensure a minimum level of personal data protection.

Section 34

(Processing by Electronic Means)

1. Processing personal data by electronic means shall only be allowed if the minimum security measures referred to below are adopted in accordance with the arrangements laid down in the technical specifications as per Annex B:

a) computerised authentication,

b) implementation of authentication credentials management procedures,

c) use of an authorisation system,

d) regular update of the specifications concerning scope of the processing operations that may be performed by the individual entities in charge of managing and/or maintenancing electronic means,

e) protection of electronic means and data against unlawful data processing operations, unauthorised access and specific software,

f) implementation of procedures for safekeeping backup copies and restoring data and system availability,

g) keeping an up-to-date security policy document,

h) implementation of encryption techniques or identification codes for specific processing operations performed by health care bodies in respect of data disclosing health and sex life.

1-bis.[6] Where an entity only processes non-sensitive personal data or else sensitive and judicial data that relate to the respective employees and collaborators, including non-EU nationals, and/or to their spouses and/or relatives, the obligation to keep an updated security policy document shall be replaced by the obligation for the data controller to issue a self-executing affidavit, in pursuance of section 47 of the consolidated statute referred to in Presidential decree no. 445 dated 28 December 2000, certifying that only the data in question are processed in compliance with the minimum security measures laid down herein as well as in the technical specifications document contained in Annex B hereto. As regards the said processing operations as well as any processing that is carried out for standard administrative and accounting purposes, in particular by SMEs, self-employed professionals, and handicrafts, the Garante shall determine, by own decision to be updated on a regular basis, having consulted with the Minister for De-Regulation and the Minister for Public Administration, simplified arrangements to implement the technical specifications contained in the said Annex B with a view taking the minimum measures mentioned in paragraph 1. [Amended by Section 6(2)a, item 5. of decree no. 70 dated 13 May 2011 as converted, with amendments, into Act no. 106 dated 12 July 2011]

1-ter. For the purpose of applying the provisions concerning the protection of personal data, a processing operation performed for administrative and accounting purposes shall by any processing operation that is related to the performance of organizational, administrative, financial and accounting activities irrespective of the nature of the processed data. The said purposes apply, in particular, to in-house organizational activities, the activities aimed at fulfilling contractual and pre-contractual obligations, managing employer-employee relationships, keeping accounting records, and implementing the legislation on taxation, trade unions, social security and welfare, and occupational health and safety. [Added by Section 6(2)a, item 5. of decree no. 70 dated 2011 as converted, with amendments, into Act no. 106 dated 12 July 2011]

Section 35

(Processing without Electronic Means)

1. Processing personal data without electronic means shall only be allowed if the minimum security measures referred to below are adopted in accordance with the arrangements laid down in the technical specifications as per Annex B:

a) regular update of the specifications concerning scope of the processing operations that may be performed by the individual entities in charge of the processing and/or by the individual organisational departments,

b) implementing procedures such as to ensure safekeeping of records and documents committed to the entities in charge of the processing for the latter to discharge the relevant tasks,

c) implementing procedures to keep certain records in restricted-access filing systems and regulating access mechanisms with a view to enabling identification of the entities in charge of the processing.

[6] Paragraph added by Section 29(1) of decree-law no. 112 dated 25 June 2008, as converted, with amendments, into Act no. 133 dated 6 August 2008.

Section 36[7]

(Upgrading)

1. The technical specifications as per Annex B concerning the minimum measures referred to in this Chapter shall be regularly updated by a decree of the Minister of Justice issued in agreement with the Minister for Innovation and Technologies and the Minister for De-Regulation by having regard to both technical developments and the experience gathered in this sector.

TITLE VI – PERFORMANCE OF SPECIFIC TASKS

Section 37

(Notification of the Processing)

1. A data controller shall notify the processing of personal data he/she intends to perform exclusively if said processing concerns:

a) genetic data, biometric data, or other data disclosing geographic location of individuals or objects by means of an electronic communications network,

b) data disclosing health and sex life where processed for the purposes of assisted reproduction, provision of health care services via electronic networks in connection with data banks and/or the supply of goods, epidemiological surveys, diagnosis of mental, infectious and epidemic diseases, seropositivity, organ and tissue transplantation and monitoring of health care expenditure,

c) data disclosing sex life and the psychological sphere where processed by not-for-profit associations, bodies or organisations, whether recognised or not, of a political, philosophical, religious or trade-union character,

d) data processed with the help of electronic means aimed at profiling the data subject and/or his/her personality, analysing consumption patterns and/or choices, or monitoring use of electronic communications services except for such processing operations as are technically indispensable to deliver said services to users,

e) sensitive data stored in data banks for personnel selection purposes on behalf of third parties, as well as sensitive data used for opinion polls, market surveys and other sample-based surveys,

f) data stored in ad-hoc data banks managed by electronic means in connection with creditworthiness, assets and liabilities, appropriate performance of obligations, and unlawful and/or fraudulent conduct.

---

[7] This paragraph was amended by Section 29(5-bis) of decree law no. 112 dated 25 June 2008, as converted, with amendments, into Act no. 133 dated 6 August 2008.

1-bis. [8] The notification relating to the data referred to in paragraph 1 shall not be required if it concerns the activity carried out by general practitioners and/or freely chosen paediatricians, as the relevant functions are typical of their professional relationships with the National Health Service.

2. The Garante may specify, by means of a decision that shall be adopted also in pursuance of Section 17, additional processing operations that are liable to affect the data subjects' rights and freedoms on account of the relevant mechanisms and/or the nature of the personal data at stake. By means of a similar decision to be published in the Official Journal of the Italian Republic, the Garante may also specify the processing operations among those referred to in paragraph 1 that are not liable to be prejudicial in the way described above and are therefore exempted from notification.

3. The notification shall be submitted by means of a single form also if the processing entails cross-border data flows.

4. The Garante shall enter the notifications submitted as above into a publicly available register of processing operations and shall set out the mechanisms for such register to be interrogated free of charge via electronic networks, also by means of agreements with public bodies or else at the Office of the Garante. Any information that is accessed by interrogating said register may only be processed for the purpose of implementing personal data protection legislation.

Section 38

(Notification Mechanisms)

1. The notification of processing operations shall have to be submitted to the Garante in advance of the processing and once only, regardless of the number of operations to be performed and the duration of the processing, and may concern one or more processing operations for related purposes.

2.[9] A notification shall only be effective if it is transmitted via the Garante's website by using the ad-hoc form, which shall contain the request to provide all the following pieces of information:

a. information to identify the data controller and, where appropriate, his/her representative, as well as the arrangements to identify the data processor if the latter has been appointed;
b. the purpose(s) of the processing;
c. a description of the category/categories of data subject and the data or data categories related to the said category/categories of data subject;
d. the data recipients or the categories of data recipient;
e. data transfers to third countries, where envisaged;
f. a general description that shall allow assessing beforehand whether the measures adopted to ensure security of the processing are adequate.

[8] This paragraph was added by Section 2-quinquies of Decree-Law no. 81 of 29th March 2004, converted into Act no. 138 of 26th May 2004.
[9] This paragraph was replaced by Section 29(4) of decree law no. 112 dated 25 June 2008, as converted, with amendments, into Act no. 133 dated 6 August 2008.

3. The Garante shall enhance both availability of the electronic form and submission of notifications also by means of agreements with authorised entities pursuant to the legislation in force, including trade associations and professional councils.

4. A new notification shall only have to be submitted either prior to termination of processing operations or in connection with the modification of any of the items to be specified in the notification.

5. The Garante may set out further appropriate arrangements for notification by having regard to new technological solutions as referred to in the legislation in force.

6. Where a data controller is not required to submit a notification to the Garante in pursuance of Section 37, he/she shall make available the information contained in the form as per paragraph 2 to any person requesting it, unless the processing operations concern public registers, lists, records or publicly available documents.

Section 39

(Communication Obligations)

1. Data controllers shall be required to communicate what follows in advance to the Garante:

a) that personal data are to be communicated by a public body to another public body in the absence of specific laws or regulations, irrespective of the form taken by such communication and also in case the latter is based on an agreement,

b) that data disclosing health are to be processed in pursuance of the biomedical or health care research programme referred to in Section 110(1), first sentence.

2. The processing operations that are the subject of a communication as per paragraph 1 may start after 45 days have elapsed since receipt of the relevant communication, except as provided otherwise by the Garante also thereafter.

3. The communication as per paragraph 1 shall be given by using the form drawn up and made available by the Garante; it shall be transmitted to the latter either electronically in compliance with the digital signature and receipt confirmation mechanisms outlined in Section 38(2), or by fac-simile or registered letter.

Section 40

(General Authorisations)

1. The provisions of this Code referring to an authorisation to be granted by the Garante shall also be implemented by issuing authorisations applying to specific categories of data controller or processing, which shall be published in the Official Journal of the Italian Republic.

Section 41

(Authorisation Requests)

1. Data controllers falling under the scope of application of an authorisation issued pursuant to Section 40 shall not be required to lodge an authorisation request with the Garante if the processing they plan to perform is compliant with the relevant provisions.

2. If an authorisation request concerns a processing operation that has been authorised pursuant to Section 40, the Garante may decide nevertheless to take steps regarding said request on account of the specific modalities of the processing.

3. Any authorisation request shall be submitted by using exclusively the form drawn up and made available by the Garante, and shall be transmitted to the latter electronically in compliance with the arrangements applying to digital signature and receipt confirmation as per Section 38(2). Said request and authorisation may also be transmitted by fac-simile or registered letter.

4. If the requesting party is called upon by the Garante to provide information or produce documents, the forty-five-day period referred to in Section 26(2) shall start running from the date of expiry of the term for complying with the above request.

5. Under special circumstances, the Garante may issue a provisional, time-limited authorisation.

TITLE VII – TRANSBORDER DATA FLOWS

Section 42

(Data Flows in the EU)

1. The provisions of this Code shall not be applied in such a way as to restrict or prohibit the free movement of personal data among EU Member States, subject to the taking of measures under this Code in case data are transferred in order to escape application of said provisions.

Section 43

(Permitted Data Transfers to Third Countries)

1. Personal data that are the subject of processing may be transferred from the State's territory to countries outside the European Union, temporarily or not and in any form and by any means whatsoever,

a) if the data subject has given his/her consent either expressly or, where the transfer concerns sensitive data, in writing;

b) if the transfer is necessary for the performance of obligations resulting from a contract to which the data subject is a party, or to take steps at the data subject's request prior to entering into a contract, or for the conclusion or performance of a contract made in the interest of the data subject;

c) if the transfer is necessary for safeguarding a substantial public interest that is referred to by laws or regulations, or else that is specified in pursuance of Sections 20 and 21 where the transfer concerns sensitive or judicial data;

d) if the transfer is necessary to safeguard a third party's life or bodily integrity. If this purpose concerns the data subject and the latter cannot give his/her consent because (s)he is physically unable to do so, legally incapable or unable to distinguish right and wrong, the consent shall be given by the entity legally representing the data subject, or else by a next of kin, a family member, a person cohabiting with the data subject or, failing these, the manager of the institution where the data subject is hosted. Section 82(2) shall apply;

e) if the transfer is necessary for carrying out the investigations by defence counsel referred to in Act no. 397 of 07.12.2000, or else to establish or defend a legal claim, provided that the data are transferred exclusively for said purposes and for no longer than is necessary therefor in compliance with the legislation in force applying to business and industrial secrecy;

f) if the transfer is carried out in response to a request for access to administrative records or for information contained in a publicly available register, list, record or document, in compliance with the provisions applying to this subject-matter;

g) if the transfer is necessary, pursuant to the relevant codes of conduct referred to in Annex A), exclusively for scientific or statistical purposes, or else exclusively for historical purposes, in connection with private archives that have been declared to be of considerable historical interest under Section 6(2) of legislative decree no. 490 of 29 October 1999, enacted to adopt the consolidated statute on cultural and environmental heritage, or else in connection with other private archives pursuant to the provisions made in said codes;

h) [Repealed].[10]

Section 44[11]

(Other Permitted Data Transfers)

1. The transfer of processed personal data to a non-EU Member State shall also be permitted if it is authorised by the Garante on the basis of adequate safeguards for data subjects' rights

a) as determined by the Garante also in connection with contractual safeguards, or else by means of rules of conduct as in force within the framework of companies all belonging to the same

[10] As amended by Section 40(2)e. of decree no. 201 dated 6 December 2011 subsequently converted, with amendments, into Act no. 214 dated 22 December 2011; the amendment repealed letter h. of this paragraph, which read as follows: "if the processing concerns data relating to legal persons, bodies or associations."

[11] Letter a. of this paragraph was amended by section 29(5-bis) of decree law no. 112 dated 25 June 2008, as converted, with amendments, into Act no. 133 dated 6 August 2008.

group. A data subject may establish his/her rights in the State's territory as set forth by this Code also with regard to non-compliance with the aforementioned safeguards.

b) as determined via the decisions referred to in Articles 25(6) and 26(4) of Directive 95/46/EC of the European Parliament and of the Council, of 24 October 1995, through which the European Commission may find that a non-EU Member State affords an adequate level of protection, or else that certain contractual clauses afford sufficient safeguards.

Section 45

(Prohibited Data Transfers)

1. Apart from the cases referred to in Sections 43 and 44, it shall be prohibited to transfer personal data that are the subject of processing from the State's territory to countries outside the European Union, temporarily or not and in any form and by any means whatsoever, if the laws of the country of destination or transit of the data do not ensure an adequate level of protection of individuals. Account shall also be taken of the methods used for the transfer and the envisaged processing operations, the relevant purposes, nature of the data and security measures.

PART II – PROVISIONS APPLYING TO SPECIFIC SECTORS

TITLE I – PROCESSING OPERATIONS IN THE JUDICIAL SECTOR

CHAPTER I – IN GENERAL

Section 46

(Data Controllers)

1. Judicial offices at all levels and of all instances, the Higher Council of the Judiciary, the other self-regulatory bodies and the Ministry of Justice shall act as controllers of the processing operations concerning personal data in connection with the tasks respectively conferred on them by laws and/or regulations.

2. The non-occasional processing operations referred to in paragraph 1 that are performed by electronic means shall be specified in a decree by the Minister of Justice as per Annex C) to this Code where they concern data banks that are either centralised or interconnected with regard to several offices and/or data controllers. The provisions by which the Higher Council of the Judiciary and the other self-regulatory bodies referred to in paragraph 1 specify the processing operations they respectively perform shall be included into Annex C) pursuant to a decree by the Minister of Justice.

Section 47

(Processing Operations for Purposes of Justice)

1. As for the processing of personal data carried out by judicial offices at all levels and of all instances, by the Higher Council of the Judiciary, other self-regulatory bodies and the Ministry of Justice, the following provisions of the Code shall not apply if the processing is carried out for purposes of justice:

a) Sections 9, 10, 12, 13 and 16, 18 to 22, 37, 38 (paragraphs 1 to 5), and 39 to 45;

b) Sections 145 to 151.

2. For the purposes of this Code, personal data shall be considered to be processed for purposes of justice if the processing is directly related to the judicial handling of matters and litigations, or if it produces direct effects on the functioning of courts as regards legal and economic status of members of the judiciary, as well as if it is related to auditing activities carried out in respect of judicial offices. Conventional administrative and management activities regarding personnel, assets or facilities shall not be considered to be carried out for purposes of justice if they do not affect the secrecy of acts that are directly related to the handling of matters and litigations referred to above.

Section 48

(Data Banks of Judicial Offices)

1. Where judicial authorities at all levels and of all instances may acquire data, information, records and documents from public bodies pursuant to the procedural regulations in force, such acquisition may also take place electronically. To that end, judicial offices may avail themselves of the standard agreements made by the Minister of Justice with public bodies in order to facilitate interrogation by said offices of public registers, lists, filing systems and data banks via electronic communication networks, whereby compliance with the relevant provisions as well as with the principles laid down in Sections 3 and 11 of this Code shall have to be ensured.

Section 49

(Implementing Provisions)

1. The regulatory provisions required to implement the principles of this Code with regard to civil and criminal matters shall be adopted by means of a decree of the Minister of Justice, which shall also supplement the provisions laid down in decree no. 334 of 30 September 1989 by the Minister of Justice

CHAPTER II – CHILDREN

Section 50

(Reports or Images Concerning Underage Persons)

1. The prohibition to publish and disseminate, by any means whatsoever, reports or images allowing an underage person to be identified, which is referred to in Section 13 of Presidential Decree no. 448 of 22 September 1988, shall also apply if an underage person is involved for whatever reason in judicial proceedings concerning non-criminal matters.

CHAPTER III – LEGAL INFORMATION SERVICES

Section 51

(General Principles)

1. Without prejudice to procedural regulations on viewing and obtaining abstracts and copies of records and documents, the data identifying matters pending before judicial authorities at all levels and of all instances shall be made accessible to any entity interested therein also by means of

electronic communications networks, including the institutional sites of said authorities on the Internet.

2. Judgments and other decisions of judicial authorities at all levels and of all instances that have been deposited with the court's clerk's office shall be made accessible also by means of the information systems and institutional sites of said authorities on the Internet, in compliance with the precautions referred to in this Chapter.

Section 52

(Information Identifying Data Subjects)

1. Without prejudice to the provisions that regulate drawing up and contents of judgments and other measures by judicial authorities at all levels and of all instances, a data subject may request on legitimate grounds, by depositing the relevant application with either the court's clerk's office or the secretariat of the authority in charge of the proceeding, prior to finalisation of the latter, that said office or secretariat add a notice to the original text of the judgment or measure to the effect that the data subject's name and other identification data as reported in the judgment or measure must not be referred to if said judgment or measure are to be reproduced in whatever form for legal information purposes on legal journals, electronic media or else by means of electronic communication networks.

2. The judicial authority issuing the judgment and/or taking the measure at stake shall decide on the request referred to in paragraph 1 by an order without further formalities. Said authority may order of its own motion that the notice as per paragraph 1 be added in order to protect data subjects' rights or dignity.

3. In the cases as per paragraphs 1 and 2, the court's clerk's office or secretariat shall add and undersign, also by stamping it, the following notice upon depositing the relevant judgment or measure, by also referring to this Section: "*In case of disclosure, leave out name(s) and other identification data concerning …*".

4. If judgments or other measures, or the corresponding headnotes, bearing the notice as per paragraph 2 are disclosed also by third parties, the data subject's name and other identification data shall be omitted.

5. Without prejudice to Section 734-bis of the Criminal Code as applying to victims of sexual violence, whoever discloses judgments or other measures by judicial authorities at all levels and of all instances shall be required to omit, in any case, name(s), other identification data and other information, also concerning third parties, that may allow detecting - directly or not - the identity of children or else of parties to proceedings concerning family law and civil status – irrespective of the absence of the notice referred to in paragraph 2.

6. The provisions of this Section shall also apply in case an award under Section 825 of the Civil Procedure Code is deposited. A party may lodge the request as per paragraph 1 with the arbitrators prior to issuing of the relevant award, and the arbitrators shall add the notice referred to in paragraph 3 to their award also in pursuance of paragraph 2. The arbitration panel set up at the Arbitration Chamber for Public Works under Section 32 of Act no. 109 of 11 February 1994 shall proceed accordingly in case a party lodges the relevant request.

7. Except for the cases referred to in this Section, the contents of judgments and other judicial measures may be disclosed in full in whatever form.

TITLE II – PROCESSING OPERATIONS BY THE POLICE

CHAPTER I – IN GENERAL

Section 53

(Scope of Application and Data Controllers)

1. The following provisions of this Code shall not apply to the processing of personal data that is carried out either by the Data Processing Centre at the Public Security Department or by the police with regard to the data that are intended to be transferred to said centre under the law, or by other public bodies or public security entities for the purpose of protecting public order and security, the prevention, detection or suppression of offences as expressly provided for by laws that specifically refer to such processing:

a) Sections 9, 10, 12, 13 and 16, 18 to 22, 37, 38(1) to (5), and 39 to 45;

b) Sections 145 to 151.

2. The non-occasional processing operations referred to in paragraph 1 as performed by electronic means and the relevant data controllers shall be specified in a decree by the Minister for Home Affairs, which shall be annexed to this Code as Annex C).

Section 54

(Processing Mechanisms and Data Flows)

1. Whenever public security authorities or the police may acquire data, information, records and documents from other entities in accordance with the laws and regulations in force, such acquisition may also take place by electronic means. To that end, the bodies or offices concerned may avail themselves of agreements aimed at facilitating interrogation by said bodies or offices, via electronic communication networks, of public registers, lists, filing systems and data banks in pursuance of the relevant provisions as well as of the principles laid down in Sections 3 and 11. Such standard agreements shall be adopted by the Minister for Home Affairs following a favourable opinion given by the Garante, and shall set out arrangements for connections and accesses also with a view to ensuring selective access exclusively to the data required to achieve the purposes referred to in Section 53.

2. The data processed for the purposes referred to in Section 53 shall be kept separately from those that are stored for administrative purposes, which do not require their use.

3. Subject to the provisions made in Section 11, the Data Processing Centre referred to in Section 53 shall be responsible for ensuring that the personal data undergoing processing are regularly updated, relevant and not excessive, also by interrogating – as authorised – the register held by the Criminal Records Office and the register of pending criminal proceedings at the Ministry of Justice pursuant to Presidential Decree no. 313 of 14 November 2002 as well as other police data banks that are required for the purposes referred to in Section 53.

4. Police bodies, offices and headquarters shall regularly verify compliance with the requirements referred to in Section 11 with regard to the data processed with or without electronic means, and shall update such data also based on the procedures adopted by the Data Processing Centre in pursuance of paragraph 3; alternatively, notices and other remarks may be added to the documents containing the processed data if the processing is carried out without electronic means.

Section 55

(Specific Technology)

1. Where the processing of personal data carries higher risks of harming data subjects by having regard, in particular, to genetic or biometric data banks, technology based on location data, data banks based on particular data processing techniques and the implementation of special technology, the measures and precautions aimed at safeguarding data subjects shall have to be complied with as required by Section 17 and prior communication shall have to be given to the Garante as per Section 39.

Section 56

(Safeguards for Data Subjects)

1. The provisions referred to in Section 10, paragraphs 3 to 5, of Act no. 121 of 1 April 1981 as subsequently amended shall also apply to data that are processed with electronic means by police bodies, offices or headquarters as well as to the data that are intended to be transferred to the Data Processing Centre referred to in Section 53.

Section 57

(Implementing Provisions)

1. A Presidential Decree issued following a resolution by the Council of Ministers, acting on a proposal put forward by the Minister for Home Affairs in agreement with the Minister of Justice, shall set out the provisions implementing the principles referred to in this Code with regard to data processing operations performed by the Data Processing Centre as well as by police bodies, offices and headquarters for the purposes mentioned in Section 53, also with a view to supplementing and amending Presidential Decree no. 378 of 3 May 1982, and by putting into practice Council of

Europe's Recommendation No. R(87)15 of 17 September 1987 as subsequently modified. Said provisions shall be set out by having regard, in particular, to

a) the principle by which data collection should be related to the specific purpose sought, in connection with preventing a concrete danger or suppressing offences, in particular as regards processing operations for analysis purposes,

b) regular updating of the data, also in connection with assessment operations carried out under the law, the different arrangements applying to data that are processed without electronic means and the mechanisms to notify the updated information to the other bodies and offices that had previously received the original data,

c) the prerequisites to carry out processing operations on transient grounds or else in connection with specific circumstances, also with a view to verifying data quality requirements as per Section 11, identifying data subject categories and keeping such data separate from other data for which they are not required,

d) setting out specific data retention periods in connection with nature of the data or the means used for processing such data as well as with the type of proceeding in whose respect they are to be processed or the relevant measures are to be taken,

e) communication of the data to other entities, also abroad, or else with a view to exercising a right or a legitimate interest, as well as to dissemination of the data, where this is necessary under the law,

f) use of specific data processing and retrieval techniques, also by means of reverse search systems.

TITLE III – STATE DEFENCE AND SECURITY

CHAPTER I – IN GENERAL

Section 58

(Applicable Provisions)

1. As regards the processing operations carried out by the entities referred to in Sections 3, 4 and 6 of Act no. 801 of 24 October 1977, as well as the data to which State secret applies under Section 12 of said Act, the provisions of this Code shall apply insofar as they are set out in Sections 1 to 6, 11, 14, 15, 31, 33, 58, 154, 160 and 169.

2. As regards the processing operations carried out by public bodies for purposes of defence or relating to State security, as expressly required by laws that specifically provide for such processing operations, the provisions of this Code shall apply insofar as they are set out in paragraph 1 as well as in Sections 37, 38 and 163.

3. The security measures relating to the data processed by the agencies as per paragraph 1 shall be laid down and regularly updated in a decree by the Prime Minister's Office in compliance with the provisions applying to this subject matter.

4. The arrangements to implement the applicable provisions of this Code with regard to categories of data, data subject, permitted processing operation and entities in charge of the processing, also with a view to updating and retaining the data, shall be laid down in a decree by the Prime Minister's Office.

TITLE IV – PROCESSING OPERATIONS IN THE PUBLIC SECTOR

CHAPTER I – ACCESS TO ADMINISTRATIVE RECORDS

Section 59

(Access to Administrative Records)

1. Subject to the provisions made in Section 60, prerequisites for, mechanisms of, and limitations on exercise of the right to access administrative records containing personal data, and the relevant judicial remedies shall be regulated further by Act no. 241 of 7 August 1990 as subsequently amended and by the other laws concerning this subject-matter, as well as by the relevant implementing regulations, also with regard to the categories of sensitive and judicial data and the processing operations that may be performed to comply with a request for access. The activities aimed at implementing the relevant provisions shall be regarded to be in the substantial public interest.

Section 60

(Data Disclosing Health and Sex Life)

1. Where the processing concerns data disclosing health or sex life, it shall be allowed if the legal claim to be defended by means of the request for accessing administrative records is at least equal in rank to the data subject's rights, or else if it consists in a personal right or another fundamental, inviolable right or freedom.

CHAPTER II – PUBLIC REGISTERS AND PROFESSIONAL REGISTERS

Section 61

(Use of Public Information)

1. The Garante shall encourage adoption, pursuant to Section 12, of a code of conduct and professional practice for processing personal data from archives, registers, lists, records or documents held by public bodies, by also specifying the cases in which the source of the data is to be mentioned and laying down suitable safeguards in connection with matching data from different archives, and by taking account of the provisions made in Council of Europe's Recommendation No. R(91)10 as regards Section 11.

2. For the purposes of implementing this Code, personal data other than sensitive or judicial data that are to be entered into a professional register pursuant to laws or regulations may be communicated to public and private bodies and disseminated also by means of electronic communication networks, in pursuance of Section 19, paragraphs 2 and 3. Reference may also be made to the existence of measures that either provide for disqualification from practising a profession or produce effects on such practice.

3. The relevant professional board or society may, at the request of the member interested therein, supplement the information referred to in paragraph 2 by additional, relevant and not excessive data in connection with professional activities.

4. At the data subject's request, the relevant professional board or society may also provide third parties with information or data concerning, in particular, professional qualifications that are not mentioned in the register, or else the availability to undertake tasks or the consent to receive scientific information materials also concerning meetings and workshops.

CHAPTER III – REGISTERS OF BIRTHS, DEATHS AND MARRIAGES, CENSUS REGISTERS AND ELECTORAL LISTS

Section 62

(Sensitive and Judicial Data)

1. The purposes consisting in keeping the registers of births, deaths and marriages, census registers for the resident population in Italy and Italian nationals resident abroad, and electoral lists, as well as in issuing identification documents or providing for name changes shall be regarded to be in the substantial public interest pursuant to Sections 20 and 21.

Section 63

(Interrogation of Records)

1. The records concerning the registers of births, deaths and marriages as kept in State Archives may be interrogated insofar as this is provided for by Section 107 of legislative decree no. 490 of 29 October 1999.

CHAPTER IV – PURPOSES IN THE SUBSTANTIAL PUBLIC INTEREST

Section 64

(Citizenship, Immigration and Alien Status)

1. For the purposes of Sections 20 and 21, the activities aimed at implementing the provisions concerning citizenship, immigration, asylum, alien and refugee status and displaced persons shall be considered to be in the substantial public interest.

2. For the purposes referred to in paragraph 1, it shall be allowed to process, in particular, sensitive and judicial data that are indispensable in order to:

a) issue visas, permits, certifications, authorizations and documents, including medical documents;
b) recognise right of asylum or refugee status, or implement temporary protection and any other humanitarian measures, or else fulfil legal obligations related to immigration policy;
c) fulfil the obligations imposed on employers and employees, allow reunification of families, implement legislation in force applying to education and housing, enable participation in public life and social integration.

3. This Section shall not apply to the processing of sensitive and judicial data that is performed to implement the agreements and conventions referred to in Section 154(2), letters a) and b), or for purposes related to State defence or security or else for preventing, detecting and suppressing offences as based on legislation that specifically provides for such processing.

Section 65

(Political Rights and Public Disclosure of the Activities of Certain Bodies)

1. For the purposes of Sections 20 and 21, the activities aimed at implementing the provisions concerning

a) electors and elected and exercise of other political rights, in compliance with secrecy of voting, and exercise of the mandate conferred on representation bodies or keeping of the general lists of jurors,
b) documentation of the institutional activities carried out by public bodies

shall be considered to be in the substantial public interest.

2. Processing of sensitive and judicial data for the purposes referred to in paragraph 1 shall be allowed in order to discharge specific tasks as laid down in laws and regulations including, in particular, those related to

a) polling operations and checks on their conformity with the law;
b) petitions for referenda, the relevant polling and checks on their conformity with the law;
c) establishing the grounds for ineligibility for or disqualification from a public office, the grounds for removal or suspension from a public office, or else for suspension or dissolution of an organ;
d) evaluation of reports, petitions, applications and community-sponsored bills, the activity of investigation committees, relationships with political groups;
e) nominating and appointing representatives in committees, bodies and offices.

3. For the purposes of this Section, it shall be allowed to disseminate sensitive and judicial data for the purposes referred to in paragraph 1, letter a), with particular regard to underwriters of electoral lists, submission of candidates, tasks conferred within political organizations or associations, institutional offices and elected organs.

4. For the purposes of this Section, in particular, it shall be allowed to process sensitive and judicial data that are indispensable

a) to draw up minutes and reports of the activity of representatives' meetings, committees and other collegiate organs or assemblies,

b) exclusively to carry out activities consisting in supervision, political guidance and inspection, and to access documents as permitted by laws and regulations concerning the relevant bodies exclusively for purposes that are directly related to discharge of an electoral mandate.

5. Sensitive and judicial data that are processed for the purposes referred to in paragraph 1 may be communicated and disseminated in accordance with the relevant legislation. It shall not be permitted to disclose sensitive and judicial data that are not indispensable to ensure compliance with the publicity principle applying to institutional activities, subject to the ban on disseminating data disclosing health.

Section 66

(Taxation and Customs Matters)

1. For the purposes of Sections 20 and 21, the activities of public bodies aimed at implementing, even through the relevant licensees, the provisions concerning taxation in respect of taxpayers and those concerning tax deductions and exemptions, as well as the activities aimed at implementing the provisions that must be enforced by customs offices, shall be considered to be in the substantial public interest.

2. Furthermore, as regards taxation matters, the activities aimed at preventing and suppressing breaches of the relevant obligations, taking the measures provided for in laws, regulations and Community legislation, checking and enforcing full compliance with said obligations, paying reimbursement, allocating taxation quotas, managing and selling State-owned property, making the

inventory of and evaluating property and keeping land registries shall be considered to be in the substantial public interest for the purposes of Sections 20 and 21.

Section 67

(Auditing and Controls)

1. For the purposes of Sections 20 and 21, the activities aimed at

a) verifying lawfulness, fairness and impartiality of administrative activities and compliance of the latter with rational, cost-effective, and efficient criteria, in the light of the fact that public bodies are anyhow entrusted by law with control, verification and inspection tasks concerning other entities,

b) inquiring into sensitive and judicial data, in compliance with the relevant institutional purposes, with regard to complaints and petitions as well as to the controls and inspections referred to in Section 65(4)

shall be regarded to be in the substantial public interest.

Section 68

(Grants and Certifications)

1. For the purposes of Sections 20 and 21, the activities aimed at implementing the provisions for granting, paying, modifying and withdrawing benefits, allowances, gifts, other types of payment and certifications shall be considered to be in the substantial public interest.

2. The processing operations falling within the scope of this Section shall also include such processing operations as are indispensable with regard to:

a) communications, certificates and information provided for in anti-Mafia legislation;
b) granting allowances as laid down in laws and regulations concerning extortion and victims of extortion;
c) payment of war pensions and granting benefits to victims of political persecution and persons detained in concentration camps as well as to their relatives;
d) granting disability claims;
e) granting allowances in connection with vocational training;
f) granting allowances, funds, gifts and further benefits as laid down in laws, regulations and Community legislation as also related to associations, foundations and other bodies;
g) granting exemptions, allowances or price reductions, and tax allowances, or else licences also in the broadcasting sector, permits, authorisations, registrations and further certifications as provided for by laws, regulations and Community legislation.

3. Processing may also include dissemination if this is indispensable to ensure transparency of the activities referred to in this Section under the law as well for purposes of supervision and control in connection with said activities, subject to the ban on dissemination of data disclosing health.

Section 69

(Granting Honours, Rewards and Recognition)

1. For the purposes of Sections 20 and 21, the activities aimed at implementing the provisions for granting honours and rewards, recognising legal personality of associations, foundations and other bodies, including religious denominations, assessing – to the extent this falls within the competence of a public body – moral character and professional qualifications for appointment to an office, including an ecclesiastical office, or to management posts in corporations, businesses and non-public schooling institutions, as well as for granting and withdrawing authorizations or certifications, granting sponsorship, patronage and symbolic prizes, participating in boards of honours and getting access to official ceremonies and meetings shall be considered to be in the substantial public interest.

Section 70

(Voluntary Organisations and Conscientious Objection)

1. For the purposes of Sections 20 and 21, the activities aimed at implementing the provisions concerning relationships between public entities and voluntary organizations – in particular as regards granting funds for their support, keeping the general registers of said organizations and international cooperation – shall be considered to be in the substantial public interest.

2. The activities aimed at implementing Act no. 230 of 08.07.98 and further legislation applying to conscientious objection shall also be considered to be in the substantial public interest.

Section 71

(Imposition of Sanctions and Precautionary Measures)

1. For the purposes of Sections 20 and 21, the activities aimed at

a) implementing the provisions concerning administrative sanctions and complaints,

b) allowing exercise of the right of defence in administrative or judicial matters, also by third parties and in pursuance of Section 391-quarter of the Criminal Procedure Code, or directly at remedying miscarriages of justice, or else in case of either breach of the due process principle or unfair restriction of personal freedom,

shall be considered to be in the substantial public interest.

2. Where the processing concerns data disclosing health or sex life, it shall be allowed if the claim to establish or defend as per letter b) of paragraph 1 is at least equal in rank to the data subject's one or else if it consists in a personal right or another fundamental, inviolable right or freedom.

Section 72

(Relationships with Religious Denominations)

1. For the purposes of Sections 20 and 21, the activities aimed at managing institutional relationships with ecclesiastical bodies, religious denominations and communities shall be considered to be in the substantial public interest.

Section 73

(Other Purposes Related to Administrative and Social Matters)

1. For the purposes of Sections 20 and 21, the activities aimed at providing social assistance shall be regarded to be in the substantial public interest within the framework of the activities entrusted by law to public bodies, in particular as for

a) psychological and social support and training for youths and other entities with social, economic or family disadvantages,
b) measures – including medical care – for disadvantaged, non self-sufficient or disabled entities, including economic or home assistance services, tele-aid, personal assistance and transport services,
c) assistance to children also in connection with judicial proceedings,
d) psychological and social investigations related to national and international adoption proceedings,
e) monitoring in connection with foster care children,
f) supervision and support with regard to the stay of nomadic groups,
g) measures related to architectural barriers.

2. For the purposes of Sections 20 and 21, the following activities shall also be regarded to be in the substantial public interest within the framework of those entrusted by law to public bodies:

a) management of kindergartens,
b) management of school canteens or provision of grants, contributions and educational materials,
c) recreational initiatives and promotion of cultural and sports activities, with particular regard to organisation of holidays, exhibitions, conferences and sports events as well as to the use of immovables and occupancy of public areas,
d) provision of public housing units,
e) conscription services,
f) administrative policing, including local policing, subject to the provisions made in Section 53, with particular regard to public hygiene services and supervision over handling of corpses, and to controls concerning environment, protection of water resources and land,
g) activities carried out by public relations departments,
h) civil protection,
i) support for employee recruitment and training, in particular as regards local initiative centres for employment and one-stop employment counters,
l) regional and local ombudsmen.

CHAPTER V – SPECIFIC PERMITS

Section 74

(Car Permits and Access to Town Centres)

1. The permits issued for whatever reason to allow driving and parking vehicles serving disabled people, or else to allow driving through and parking in restricted access areas, which must be placed visibly on the relevant vehicles, shall only contain such data as are indispensable to identify the specific authorisation without using any wording that may allow identifying the natural person concerned.(1)

2. Name and address of the natural person concerned shall be reported on the said permits by taking care that they are not immediately visible unless a request is made to produce the permit or an assessment is to be carried out.(1)

3. The provision as per paragraph 2 shall also apply if the obligation to affix a copy of the car registration document or any other document on the vehicle is provided for on any grounds.

4. The provisions laid down in Presidential Decree no. 250 of 22 June 1999 shall further apply to processing of the data collected by means of equipment detecting access by vehicles to town centres and restricted access areas.

(1) As amended by Section 58 of Act no. 120 dated 29 July 2010.

TITLE V – PROCESSING OF PERSONAL DATA IN THE HEALTH CARE SECTOR

CHAPTER I – IN GENERAL

Section 75

(Scope of Application)

1. This Title shall regulate the processing of personal data in the health care sector.

Section 76

(Health Care Professionals and Public Health Care Bodies)

1. Health professionals and public health care bodies may process personal data disclosing health, also within the framework of activities in the substantial public interest pursuant to Section 85,

a) with the data subject's consent, also without being authorised by the Garante, if the processing concerns data and operations that are indispensable to safeguard the data subject's bodily integrity and health,

b) also without the data subject's consent, based on the Garante's prior authorisation, if the purposes referred to under a) concern either a third party or the community as a whole.

2. In the cases referred to in paragraph 1, consent may be given in accordance with the simplified arrangements referred to in Chapter II.

3. In the cases referred to in paragraph 1, the Garante's authorisation shall be granted after seeking the opinion of the Higher Health Care Council except for emergencies.

CHAPTER II – SIMPLIFIED ARRANGEMENTS CONCERNING INFORMATION AND CONSENT

Section 77

(Simplification)

1. This Chapter shall lay down simplified arrangements that may be applied by the entities referred to in paragraph 2

a) to inform data subjects of the personal data collected either from them or from third parties, in pursuance of Section 13, paragraphs 1 and 4,
b) to obtain data subjects' consent to the processing of personal data whenever this is required under Section 76,
c) to process personal data.

2. The simplified arrangements referred to in paragraph 1 shall be applicable

a) by public health care bodies,
b) by other private health care bodies and health care professionals,
c) by the other public entities referred to in Section 80.

Section 78

(Information Provided by General Practitioners and Paediatricians)

1. General practitioners and paediatricians shall inform data subjects of the processing of personal data in a clear manner such as to allow the items referred to in Section 13(1) to be easily understandable.

2. The information may be provided as regards the overall personal data processing operations that are required for prevention, diagnosis, treatment and rehabilitation as carried out by a general practitioner or a paediatrician to safeguard the data subject's health or bodily integrity, such activities being performed at the data subject's request or else being known to the data subject in that they are carried out in his/her interest.

3. The information may also concern personal data collected from third parties and is given preferably in writing, also by means of pocketable cards with foldable annexes, and should include at least the items specified by the Garante in pursuance of Section 13(3), which may be supplemented by additional information – also verbally – in connection with specific features of the processing.

4. Unless specified otherwise by the general practitioner or paediatrician, the information shall also concern data processing operations that are related to those carried out by said general practitioner or paediatrician, being performed by either a professional or another entity, who should be identifiable on the basis of the service requested and

a) temporarily replaces the general practitioner or paediatrician in question,

b) provides specialised advice at the general practitioner's or paediatrician's request,

c) may lawfully process the data within the framework of a professional partnership,

d) supplies prescribed drugs,

e) communicates personal data to the general practitioner or paediatrician in compliance with the applicable regulations.

5. The information provided pursuant to this Section shall highlight, in detail, processing operations concerning personal data that may entail specific risks for the data subject's rights and fundamental freedoms and dignity, in particular if the processing is carried out

a) for scientific purposes, including scientific research and controlled clinical drug testing, in compliance with laws and regulations, by especially pointing out that the consent, if necessary, is given freely,

b) within the framework of tele-aid or tele-medicine services,

c) to supply other goods or services to the data subject via electronic communication networks.

Section 79

(Information Provided by Health Care Bodies)

1. Public and private health care bodies may avail themselves of the simplified arrangements concerning information and consent referred to in Sections 78 and 81 with regard to several services delivered also by different divisions and units of a selfsame body or else by several specifically identified hospitals and local entities.

2. In the cases referred to in paragraph 1, the health care body or entity shall record the provision of information and consent in a unified manner such as to allow this circumstance to be verified by other divisions and units that may happen to process data concerning the same data subject also thereafter.

3. The simplified arrangements referred to in Sections 78 and 81 may be applied in a homogeneous, consistent manner with regard to all the processing operations concerning personal data that are carried out by all the entities pertaining to a given health care agency.

4. Based on appropriate organisational measures in pursuance of paragraph 3, the simplified arrangements in question may be applied to several data processing operations carried out both in the cases referred to in this Section and by the entities referred to in Section 80.

Section 80

(Information Provided by Other Public Bodies)

1. In addition to the provisions made in Section 79, the competent services or departments of public bodies working in the sectors of health care and/or occupational safety and prevention may avail themselves of the possibility to provide a single information notice in connection with several data processing operations performed in different periods for administrative purposes with regard to data collected both from a data subject and from third parties.

2. The information as per paragraph 1 shall be supplemented by placing suitable, specific notices and signs, which shall be easily visible to the public and shall be affixed and disseminated also within the framework of institutional publications as well as on electronic communication networks – with particular regard to administrative activities in the substantial public interest requiring no consent by data subjects.

Section 81

(Providing One's Consent)

1. Consent to the processing of data disclosing health – where required pursuant to either this Code or another law – may be provided by means of a single statement, also verbally. In this case, the consent shall not be documented in a written instrument released by the data subject, but in a notice written by the health care professional and/or public health care body, in which reference shall be made to the processing of data by either one or several entities and to the information provided to the data subject according to Sections 78, 79 and 80.

2. Where a general practitioner or paediatrician provides information on behalf of several professionals as per Section 78 (4), the consent rendered in pursuance of paragraph 1 shall have to be also notified to said professionals by appropriate mechanisms, also by referring to it or placing a notice or a stamp/tag on a electronic card and/or the medical card, in which reference shall be made to Section 78(4) as well as to the detailed specifications made, if any, in the information provided pursuant to the latter paragraph.

Section 82

(Emergency and Protection of Health and Bodily Integrity)

1. Information and consent requirements in connection with the processing of personal data may be complied with after the relevant service has been delivered, without delay, in cases of medical emergency and/or related to public hygiene whenever the competent authority has issued a contingent emergency order pursuant to Section 117 of legislative decree no. 112 of 31 March 1998.

2. Information and consent requirements in connection with the processing of personal data may also be complied with after the relevant service has been delivered, without delay,

a) if the data subject is physically impaired, legally incapable or unable to distinguish right and wrong, and the consent cannot be obtained from the entity legally representing the data subject, or else a next of kin, a family member, a person cohabiting with the data subject or, failing these, the manager of the institution where the data subject is hosted,

b) if there exists a serious, impending and irretrievable danger for the data subject's health or bodily integrity.

3. Information and consent requirements in connection with the processing of personal data may be complied with after the relevant service has been delivered, without delay, also if the provision of medical care may be negatively affected - in terms of its timeliness or effectiveness - by the need to obtain the data subject's prior consent.

4. As regards persons over eighteen years of age, the information shall be provided to a data subject also for the purpose of newly obtaining his/her consent whenever the latter is required.

Section 83

(Other Provisions to Ensure Respect for Data Subjects' Rights)

1. The entities referred to in Sections 78, 79 and 80 shall take suitable measures to ensure that data subjects' rights, fundamental freedoms and dignity, as well as professional secrecy requirements are respected in organising the relevant services and discharging the relevant tasks, without prejudice to the provisions made in laws and regulations concerning arrangements to process sensitive data and minimum security measures.

2. The measures referred to in paragraph 1 shall include, in particular,

a) solutions aimed at respecting precedence and order in calling up data subjects regardless of their specific names as regards medical care activities and administrative requirements entailing a waiting time,

b) setting up appropriately spaced waiting lines by having regard to the use of voice messages and/or barriers,

c) solutions to prevent third parties from unduly getting to know information disclosing health during an interview,

d) precautions aimed at preventing medical care activities – including collection of a patient's history – from being carried out in privacy-unfriendly situations due to the specific arrangements and/or the premises selected,

e) respect for the data subject's dignity when providing the specific medical treatment as well as in connection with all data processing operations,

f) suitable arrangements to ensure that the provision of emergency aid can be notified or confirmed also by phone, if necessary, exclusively to third parties entitled thereto,

g) provisions in line with the internal regulations of hospitals and other establishments for medical care by which suitable mechanisms are laid down to inform third parties that are lawfully entitled thereto on the whereabouts of data subjects inside medical wards, on the occasion of visits paid by such third parties, whereby data subjects are informed thereof in advance and compliance with their legitimate denial of authorisation is ensured,

h) implementing procedures, including training of staff, to prevent third parties from establishing a link between a data subject and a given ward or department such as to disclose a specific medical condition,

i) subjecting persons in charge of the processing that are not bound by professional secrecy under the law to rules of practice that are similar to those based on professional secrecy.

2-bis. [12] The measures referred to in paragraph 2 shall not apply to the entities as per Section 78, who shall comply with the provisions set out in paragraph 1 by such mechanisms as are suitable for ensuring personalised, trust-based relationships with their patients pursuant to the code of conduct and professional practice adopted under Section 12 hereof.

Section 84

(Data Communication to Data Subjects)

1. Personal data disclosing health may be communicated by health care professionals and health care bodies either to the data subject or to the entities referred to in Section 82(2), letter a), only by the agency of a physician who must have been designated either by the data subject or by the data

[12] This paragraph was added by Section 2-quinquies, paragraph 1, letter b., of Decree-Law no. 81 of 29th March 2004, converted with amendments into Act no. 138 of 26th May 2004.

controller. This paragraph shall not apply to the personal data that had been provided previously by said data subject.

2. The data controller or processor may authorise, in writing, health care professionals other than physicians who, to fulfil their respective duties, have direct contacts with patients and are in charge of processing personal data disclosing health, to communicate said data either to data subjects or to the entities referred to in Section 82(2), letter a). The instrument by which said task is conferred shall set out adequate arrangements and precautions having regard to the context within which the data are to be processed.

CHAPTER III – PURPOSES IN THE SUBSTANTIAL PUBLIC INTEREST

Section 85

(Tasks of the National Health Service)

1. Except for the cases referred to in paragraph 2, the activities falling within the scope of the tasks committed to the National Health Service and other public health care bodies shall be considered to be in the substantial public interest for the purposes of Sections 20 and 21 as regards:

a) administrative activities related to prevention, diagnosis, care and rehabilitation of the persons assisted by the National Health Service, including aliens in Italy and Italian citizens abroad as well as the health care provided to seamen and airport staff;
b) planning, management, control and assessment of health care;
c) monitoring of testing and drugs, authorization for marketing and importing medical drugs and other health-related products;
d) certification activities;
e) application of provisions concerning occupational hygiene and safety and population health and safety;
f) administrative activities related to organ and tissue transplantations and human blood transfusions, also pursuant to Act no. 107 of 04.05.90;
g) setting up, managing, planning and monitoring the relationships between the administration and the entities bound by contractual agreements with and/or recognised by the National Health Service.

2. Paragraph 1 shall not apply to the processing of data disclosing health that is carried out either by health care professionals or by public health care bodies for the purpose of protecting health or bodily integrity of a data subject, a third party or the community as a whole, in which case the provisions concerning the data subject's consent and/or authorisation by the Garante shall apply as per Section 76.

3. The specification of the categories of data disclosing health and the processing operations they may undergo shall be publicised to the greatest possible extent, also by affixing a copy thereof or making available an explanatory booklet in each health care agency as well as in general practitioners' and paediatricians' clinics.

4. Processing the data subject's identification data shall be lawfully reserved for the entities that directly pursue the purposes referred to in paragraph 1. Utilisation of the various data categories shall only be allowed to the persons in charge of the processing who have been entrusted, on a case-

by-case basis, with the specific stages of the activities mentioned in paragraph 1 in accordance with the principle that only indispensable data shall have to be processed in the individual cases.

Section 86

(Other Purposes in the Substantial Public Interest)

1. Apart from the cases referred to in Sections 76 and 85, the purposes to be achieved by processing sensitive and judicial data in connection with administrative activities related to implementation of the legislation concerning the matters below shall be regarded to be in the substantial public interest as per Sections 20 and 21:

a) social protection of motherhood and abortion, with particular regard to the processing operations that are carried out for managing family planning centres and similar institutions, providing information, medical treatment and in-hospital care to mothers, as well as for performing abortions;

b) narcotic drugs and psychotropic substances, with particular regard to the activities carried out in order to provide, also with the help of non-profit bodies and associations, such public services as are necessary for the social and medical assistance of drug addicts, and to adopt the measures, including preventive measures, referred to by laws and implement the required administrative provisions;

c) assistance, social integration and rights of persons with a disability, in particular with a view to

1) assessing the disability and ensuring operation of medical care and rehabilitation services and family and personal support, as well as granting allowances and further benefits,
2) ensuring social integration, education, training and information to the family of a person with a disability as well as mandatory employment of such person in the cases provided for by law,
3) setting up residential facilities and social rehabilitation centres,
4) keeping the registers of voluntary bodies, associations and organisations working in this sector.

2. The provisions as per Section 85(4) shall apply to the processing operations referred to in this Section.

CHAPTER IV – MEDICAL PRESCRIPTIONS

Section 87

(Drugs Paid for by the National Health Service)

1. Prescriptions concerning medical drugs that are charged, even only in part, to the National Health Service shall be written by using the form referred to in paragraph 2. Said form shall be designed so as to allow establishing the data subject's identity only if this is necessary in order to check that the prescription is correct or else with a view to administrative controls or for epidemiological and research purposes, in compliance with the applicabile rules of conduct.

2. The paper form to be used for prescribing drugs that are charged, even only in part, to the National Health Service as per Annexes 1, 3, 5 and 6 to decree no. 350 by the Minister of Health of 11 July 1988 and Chapter 2, paragraph 2.2.2. of the relevant technical specifications, shall be supplemented either by a paper tag or by a carbon-copy tag that shall be pasted to the margins of the areas referred to in paragraph 3.

3. The tag referred to in paragraph 2 shall be affixed to the areas of the form where the patient's name and address are to be entered so that the latter may only be visible upon transiently removing the tag for the purposes specified in paragraphs 4 and 5.

4. The tag may be transiently removed from the prescription form and subsequently re-affixed to it if this is considered indispensable by a chemist – who shall have to sign the tag – on account of the actual need to check that the prescription is correct as also related to supply of the drug specifically prescribed.

5. The tag may also be transiently removed in the manner described in paragraph 3 by the competent bodies with a view to performing an administrative audit as to correctness of the prescription, and by entities that may lawfully carry out epidemiological surveys or else researches in accordance with the law, provided that this is indispensable in order to achieve their respective purposes.

6. Further technical solutions other than the one referred to in paragraph 1 may be laid down in a decree by the Minister of Health, after seeking the Garante's opinion, based on the use of a sticker or else on equivalent technology also related to the use of non-paper media.

Section 88

(Drugs Not Paid for by the National Health Service)

1. The data subject's name shall not be specified in the prescriptions made on paper forms with regard to drugs that are not charged, even in part, to the National Health Service.

2. In the cases referred to in paragraph 1, a physician may specify the data subject's name exclusively if he/she considers that it is indispensable to make said data subject personally identifiable on account of an actual requirement that is related either to the data subject's specific condition or to the special arrangements to be made for preparing or using the drug.

Section 89

(Special Cases)

1. The provisions of this Chapter shall leave unprejudiced the application of regulatory provisions requiring drug prescriptions not to allow identification of data subjects or else to bear specific notices, such as those laid down in decree-law no. 23 of 17 February 1998 as converted, with amendments, into Act no. 94 of 8 April 1998.

2. Whenever the data subject's identity is to be established in pursuance of the consolidated text of the Act applying to narcotic drugs and psychotropic substances, prevention, care and rehabilitation of drug addiction, as approved by presidential decree no. 309 of 9 October 1990, the relevant prescriptions shall be kept separate from any other document that does not require their use.

2-bis. [13] As for the entities referred to in Section 78, implementing the provisions set out in Sections 87(3) and 88(1) shall be conditional upon the data subject's explicit request.

CHAPTER V – GENETIC DATA

Section 90

(Processing of Genetic Data and Bone Marrow Donors)

1. Processing of genetic data, regardless of the entity processing them, shall be allowed exclusively in the cases provided for in ad-hoc authorisations granted by the Garante, after having consulted with the Minister for Health who shall seek, to that end, the opinion of the Higher Health Care Council.

2. The authorisation referred to in paragraph 1 shall also specify the additional items of information that should be contained in the information notice pursuant to Section 13, with particular regard to the purposes sought and the results to be achieved also in connection with the unexpected information that may be made known on account of the processing as well as with the data subject's right to object to the processing on legitimate grounds.

3. Under Act no. 52 of 6 March 2001, bone marrow donors shall have the right and duty to remain anonymous with regard to both recipient(s) and third parties.

CHAPTER VI – MISCELLANEOUS PROVISIONS

Section 91

(Data Processed by Means of Cards)

1. Processing in whatever form of data disclosing health and sex life that are stored on cards, including non-electronic cards and the national services card, or that are processed by means of said cards, shall only be allowed if it is necessary under the terms of Section 3 in compliance with measures and precautions laid down by the Garante as per Section 17.

[13] This paragraph was added by Section 2-quinquies, paragraph 1, letter c., of Decree-Law no. 81 of 29th March 2004, converted with amendments into Act no. 138 of 26th May 2004.

Section 92

(Clinical Records)

1. Where public and private health care bodies draw up and retain clinical records in compliance with the applicable legislation, suitable precautions shall be taken to ensure that the data are understandable as well as to keep the data concerning a patient separate from those concerning other data subjects – including the information related to unborn children.

2. Any request to inspect or obtain a copy of the clinical records and the attached patient discharge form as lodged by entities other than the data subject may only be granted, in whole or in part, if it is justified because of the proven need

a) to establish or defend a legal claim in pursuance of Section 26(4), letter c), such claim being equal in rank to the data subject's right or else consisting in a personal right or another fundamental, inviolable right or freedom,

b) to establish a legally relevant claim in pursuance of the legislation concerning access to administrative records, such claim being equal in rank to the data subject's right or else consisting in a personal right or another fundamental, inviolable right or freedom.

Section 93

(Certificate of Attendance at Birth)

1. With a view to issuing a birth certificate, the certificate of attendance at birth shall be replaced by a declaration only containing the data that must be entered into the register of births. The provisions of Section 109 shall also apply.

2. The certificate of attendance at birth or clinical records, where containing personal data allowing identification of a mother that has objected to being referred to as per Section 30(1) of Presidential Decree no. 396 of 3 November 2000, may be issued in full to any person interested therein, pursuant to law, after one hundred years have elapsed since the relevant document has been drawn up.

3. During the period referred to in paragraph 2, a request for accessing the certificate and/or clinical records may be granted with regard to the data concerning a mother that has objected to being referred to by taking suitable precautions to prevent the latter from being identifiable.

Section 94

(Data Banks, Registers and Filing Systems in the Health Care Sector)

1. The processing of data disclosing health as contained in data banks, filing systems, archives or registers kept by entities in the health care sector shall be carried out in compliance with Section 3 also with regard to data banks, filing systems, archives or registers that had already been set up on

the date of entry into force of this Code as well as in respect of the access by third parties pursuant to the provisions in force on that date – in particular concerning

a) the national register of asbestos-related mesotheliomas set up at the Istituto superiore per la prevenzione e la sicurezza del lavoro (Ispesl), which is referred to in Section 1 of Prime Minister's decree no. 308 of 10 December 2002,

b) the data bank on surveillance of Creutzfeldt-Jakob's disease and the variants or related syndromes, which is referred to in a decree by the Minister of Health of 21 December 2001 published in the Official Journal no. 8 of 10 January 2002,

c) the national register of rare diseases referred to in Section 3 of decree no. 279 of 18 May 2001 by the Minister of Health,

d) the registers of bone marrow donors set up in pursuance of Act no. 52 of 6 March 2001,

e) the files concerning blood donors referred to in Section 15 of a decree by the Minister of Health of 26 January 2001, as published in the Official Journal no. 78 of 3 April 2001.

TITLE VI – EDUCATION

CHAPTER I – IN GENERAL

Section 95

(Sensitive and Judicial Data)

1. For the purposes of Sections 20 and 21, the activities aimed at education and training in the schooling, vocational, high school or university sectors shall be considered to be in the substantial public interest with particular regard to those carried out also in integrated fashion.

Section 96

(Processing of Data Concerning Students)

1. With a view to facilitating vocational orientation and training as well as employment in Italy and abroad, high schools and similar educational bodies may communicate or disseminate, also to private entities and by electronic means, on the data subjects' request, data on the evaluation and marks obtained by students (whether at mid-term or in the final term) and further personal data other than sensitive or judicial data, provided they are relevant in respect of the above purposes and are referred to in the information provided to data subjects pursuant to Section 13. The data may be processed further exclusively for the abovementioned purposes.

2. The provisions referred to in Section 2(2) of Presidential Decree no. 249 of 24 June 1998 concerning protection of students' right to privacy as well as the provisions in force concerning

publication of examination marks by affixing a notice on the school's bulletin board, and those concerning the granting of diplomas and certifications shall be left unprejudiced.

TITLE VII – PROCESSING FOR HISTORICAL, STATISTICAL OR SCIENTIFIC PURPOSES

CHAPTER I – IN GENERAL

Section 97

(Scope of Application)

1. This Title shall regulate processing of personal data for historical, statistical or scientific purposes.

Section 98

(Purposes in the Substantial Public Interest)

1. For the purposes of Sections 20 and 21, the purposes related to the data processing operations carried out by public bodies

a) for historical purposes in respect of keeping, classifying and communicating the documents and records kept in State archives and historical archives of public bodies pursuant to legislative decree no. 490 of 29 October 1999, which adopted the consolidated statute on cultural and environmental heritage, as amended by this Code,

b) that are members of the National Statistical System (SISTAN) as per legislative decree no. 322 of 6 September 1989, as subsequently amended,

c) for scientific purposes,

shall be considered to be in the substantial public interest.

Section 99

(Compatibility between Purposes and Duration of Processing)

1. Processing of personal data for historical, scientific or statistical purposes shall be considered to be compatible with the different purposes for which the data had been previously collected or processed.

2. Processing of personal data for historical, scientific or statistical purposes may be carried out also upon expiry of the period that is necessary for achieving the different purposes for which the data had been previously collected or processed.

3. Where the processing of personal data is terminated, for whatever reason, such data may be kept or transferred to another data controller for historical, statistical or scientific purposes.

Section 100

(Data Concerning Studies and Researches)

1. In order to encourage and support research and co-operation in the scientific and technological sectors, public bodies including universities and research institutions may, by autonomous decision, communicate and disseminate, also to private bodies and by electronic means, data concerning studies and researches to graduates, post-graduates, technicians and engineers, researchers, professors, experts and scholars – except for sensitive and judicial data.

2. The data subject's right to object on legitimate grounds pursuant to Section 7(4), letter a), shall be left unprejudiced.

3. The data referred to in this Section shall not be regarded as administrative records under the terms of Act no. 241 of 7 August 1990.

4. The data referred to in this Section may be processed further exclusively for the purposes for which they have been communicated or disseminated.

CHAPTER II – PROCESSING FOR HISTORICAL PURPOSES

Section 101

(Processing Arrangements)

1. No personal data that has been collected for historical purposes may be used for taking actions or issuing provisions against the data subject in administrative matters, unless said data are also used for other purposes in compliance with Section 11.

2. Any document containing personal data that is processed for historical purposes may only be used, by having regard to its nature, if it is relevant and indispensable for said purposes. Personal data that are disseminated may only be used for achieving the aforementioned purposes.

3. Personal data may be disseminated in any case if they relate to circumstances or events that have been made known either directly by the data subject or on account of the latter's public conduct.

Section 102

(Code of Conduct and Professional Practice)

1. The Garante shall encourage adoption of a code of conduct and professional practice by the private and public entities, including scientific societies and professional associations, which are involved in the processing of data for historical purposes, in pursuance of Section 12.

2. The code of conduct and professional practice referred to in paragraph 1 shall set out, in particular,

a) rules based on fairness and non-discrimination in respect of users, to be abided by also in communication and dissemination of data, pursuant to the provisions of this Code that are applicable to the processing of data for journalistic purposes or else for publication of papers, essays and other intellectual works also in terms of artistic expression;

b) the specific safeguards applying to collection, interrogation and dissemination of documents concerning data disclosing health, sex life or private family relations; the cases shall be also specified in which either the data subject or an interested party must be informed by the user of the planned dissemination;

c) arrangements to apply the provisions on processing of data for historical purposes to private archives, as also related to harmonisation of interrogation criteria and the precautions to be taken in respect of communication and dissemination.

Section 103

(Interrogating Documents Kept in Archives)

1. Interrogation of documents kept in State archives, historical archives of public bodies and private archives shall be regulated by legislative decree no. 490 of 29 October 1999, enacting the consolidated Act on cultural and environmental heritage, as amended by this Code.

CHAPTER III – PROCESSING FOR STATISTICAL OR SCIENTIFIC PURPOSES

Section 104

(Scope of Application and Identification Data for Statistical or Scientific Purposes)

1. The provisions of this Chapter shall apply to the processing of data for statistical purposes or, to the extent that they are compatible, for scientific purposes.

2. For the purpose of implementing this Chapter, account shall be taken with regard to identification data of all the means that can be reasonably used by a data controller or others to identify the data subject, also on the basis of the knowledge acquired in connection with technological developments.

Section 105

(Processing Arrangements)

1. No personal data that is processed for statistical or scientific purposes may be used for taking decisions or measures with regard to the data subject or else with a view to processing data for different purposes.

2. Statistical or scientific purposes shall have to be specified unambiguously and made known to the data subject in accordance with Section 13, as also related to Section 106(2), letter b), of this Code and Section 6-bis of legislative decree no. 322 of 06.09.89 as subsequently amended.

3. Where specific circumstances referred to in the codes as per Section 106 are such as to allow an entity to respond on behalf of another entity, being a family member of or co-habiting with the latter, the data subject may also be informed by the agency of the respondent.

4. As for processing operations for statistical or scientific purposes concerning data collected for other purposes, no information shall have to be provided to data subjects if it entails a disproportionate effort compared with the right to be protected – on condition that those operations have been appropriately publicized as laid down in the Codes referred to in Section 106.

Section 106

(Codes of Conduct and Professional Practice)

1. The Garante shall encourage adoption of one or more codes of conduct and professional practice by the private and public entities, including scientific societies and professional associations, which are involved in the processing of data for statistical or scientific purposes, in pursuance of Section 12

2. The codes referred to in paragraph 1 shall lay down, by having regard to legislative decree no. 322 of 06.09.89, as subsequently amended, in respect of the entities that are members of the National Statistical System and on the basis of similar safeguards in respect of other entities,

a) prerequisites and procedures for proving and verifying that the data are processed actually for appropriate statistical and scientific purposes, except as provided for in legislative decree no. 322 of 06.09.89;

b) where not provided for in this Code, further prerequisites for the processing and the relevant safeguards, as also related to the data retention time, the information to be provided to data subjects in respect of the data collected also from third parties, communication and dissemination of the data, the selective criteria to be implemented in processing identification data, the specific security measures and the mechanisms to amend the data as a result of the exercise of data subjects' rights, by taking account of the principles laid down in the relevant Council of Europe’s Recommendations;

c) the means that can be reasonably used by data controllers or others in order to identify a data subject, by taking also account of technical developments;

d) the safeguards to be afforded with a view to applying the provisions referred to in Sections 24(1), letter I) and 43(1), letter g), making the data subject's consent unnecessary, by having regard to the principles laid down in the aforementioned Recommendations;

e) simplified arrangements for obtaining the data subjects' consent in connection with processing sensitive data;

f) the fairness criteria applying to collection of the data and the instructions for the staff in charge of this activity;

g) the measures to be adopted in order to promote compliance with the principle that the data should be relevant and not excessive as well as with the security measures referred to in Section 31, by having also regard to the precautions to be taken in order to prevent both access by natural persons who are not in charge of the processing and unauthorized identification of data subjects, the interconnection of information systems also within the framework of the National Statistical System and the data exchanges for statistical and scientific purposes that are carried out with entities and agencies abroad also based on the safeguards referred to in Section 44(1), letter a);

h) the requirement for any person in charge of the processing who is not bound by official or professional secrecy under the law to abide by rules of conduct that can ensure similar security and confidentiality levels.

Section 107

(Processing of Sensitive Data)

1. Without prejudice to Section 20 and except for specific statistical or scientific research investigations or surveys that are provided for by law, the data subject’s consent for processing sensitive data may be given, if required, in accordance with simplified arrangements as set out in the code referred to in Section 106. The relevant authorisation may be granted by the Garante also in pursuance of Section 40.

Section 108

(National Statistical System)

1. Processing of personal data by entities included in the National Statistical System shall be regulated further by legislative decree no. 322 of 6 September 1989 as subsequently amended as well as by the provisions set out in the code of conduct and professional practice adopted pursuant to Section 106(2), with particular regard to processing of the sensitive data referred to in the national statistical programme, provision of information to data subjects, exercise of data subjects’ rights and data falling outside the scope of statistical secrecy under Section 9(4) of the aforementioned decree.

Section 109

(Statistical Data Concerning Birth Events)

1. The collection of statistical data concerning birth events - including malformed newborns and stillborns - and the data flows also by medical directors shall be regulated by the technical specifications made by the National Statistics Institute after hearing the Minister of Health, the Minister of Justice and the Garante as well as by the provisions laid down in decree no. 349 of 16 July 2001 by the Minister of Health.

Section 110

(Medical, Biomedical and Epidemiological Research)

1. The data subject's consent shall not be required for processing data disclosing health with a view to scientific research activities in the medical, bio-medical or epidemiological sectors if said research activities are expressly provided for by legislation that specifically refers to the processing, or else are included in a bio-medical or health care research programme pursuant to Section 12-bis of legislative decree no. 502 of 30.12.92, as subsequently amended, and forty-five days have elapsed since communication of said activities to the Garante under Section 39. Additionally, consent shall not be necessary if data subjects cannot be informed on specific grounds and the research programme has been the subject of a reasoned, favourable opinion by the geographically competent ethics committee as well as being authorised by the Garante also in pursuance of Section 40.

2. Where a data subject exercises his/her rights in pursuance of Section 7 with regard to the processing operations which are referred to in paragraph 1, updates, rectifications and additions to the data shall be reported without modifying the data themselves if the outcome of the above operations does not produce significant effects on the outcome of the research.

TITLE VIII – OCCUPATIONAL AND SOCIAL SECURITY ISSUES

CHAPTER I – IN GENERAL

Section 111

(Code of Conduct and Professional Practice)

1. The Garante shall encourage adoption, pursuant to Section 12, of a code of conduct and professional practice by public and private entities that are involved in the processing of personal data either for social security purposes or in connection with management of employer-employee relationships, by also setting forth specific arrangements to inform data subjects and obtain their consent, if necessary, as regards publishing job ads pursuant to Section 113(3) and receiving CVs including personal – possibly sensitive – data.

Section 112

(Purposes in the Substantial Public Interest)

1. For the purposes of Sections 20 and 21, the activities carried out by public bodies in order to enter into and manage labour relations of any kind whatsoever, whether based on a contract of service or for services, including unpaid, honorary, part-time or temporary work, as well as other types of employment which do not entail any contract of service, shall be considered to be in the substantial public interest.

2. The processing operations performed for the purposes referred to in paragraph 1 shall include, in particular, those aimed at:

a) implementing the provisions concerning mandatory employment of disabled persons and employing staff also from disadvantaged groups;

b) ensuring equal opportunity policies;

c) establishing existence of specific qualifications as required to fill certain positions, as also related to protection of language minorities, or else of prerequisites for suspension from or termination of employment or service, relocation of an employee for incompatibility and granting special authorizations;

d) fulfilling obligations related to assessment of legal and economic status, including recognition of industrial accidents or granting of fair compensation, as well as obligations concerning wages, taxation or accounting in respect of staff, whether employed or retired, including payment of premia and security benefits;

e) fulfilling specific obligations or discharging tasks which are laid down in legislation concerning occupational hygiene and safety, population health and safety and trade-unions' activities;

f) implementing, as also related to social security and assistance organizations, the provisions concerning social security and assistance, including supplementary social security schemes, pursuant to, inter alia, legislative decree no. 804 of 29.07.47, with regard to communication of the data, also by means of electronic communications networks, to social assistance agencies, trade associations and professional councils that have obtained the data subject's consent under Section 23 in connection with specific data categories;

g) carrying out activities aimed at establishing civil, disciplinary and accounting liability and dealing with complaints in administrative matters pursuant to the relevant rules;

h) entering an appearance in court by the agency of counsel or else taking part in arbitration or settlement proceedings as provided for by law or collective labour agreements;

i) protecting the data subject's or a third party's life or bodily integrity;

l) managing the register of civil servants and implementing the provisions concerning tasks undertaken by civil servants, co-operators and advisors;

m) implementing the provisions concerning conflicts of interest and part-time jobs;

n) carrying out inquiries and inspections with regard to public bodies;

o) assessing quality of the services provided as well as of the results achieved.

3. The data referred to in letters m), n) and o) of paragraph 2 may be disseminated in anonymous form and anyhow in a way preventing the data subject from being identified.

CHAPTER II – JOB ADS AND EMPLOYEE DATA

Section 113

(Data Collection and Relevance)

1. The provisions laid down in Section 8 of Act no. 300 of 20 May 1970 shall be left unprejudiced.

CHAPTER III – BAN ON DISTANCE MONITORING AND TELEWORK

Section 114

(Distance Monitoring)

1. The provisions made in Section 4 of Act no. 300 of 20 May 1970 shall be left unprejudiced.

Section 115

(Telework and Home-Based Work)

1. In the context of home-based work and telework, employers shall be required to ensure that the employees' personality and moral freedom are respected.

2. Home-based workers shall be required to ensure confidentiality as necessary with regard to all family-related matters.

CHAPTER IV – ASSISTANCE BOARDS AND SOCIAL WORK

Section 116

(Availability of Data under the Terms Agreed upon with Data Subjects)

1. Assistance and social work boards may access the data banks of the entities providing the relevant services under the terms agreed upon with data subjects, in order to discharge their respective tasks, as regards the data categories that have been referred to specifically upon obtaining the data subjects' consent in pursuance of Section 23.

2. Guidelines for ad-hoc agreements to be made between assistance and social work boards and the entities providing the relevant services shall be set out in a decree by the Minister of Work and Social Policies.

TITLE IX – BANKING, FINANCIAL AND INSURANCE SYSTEMS

CHAPTER I – INFORMATION SYSTEMS

Section 117

(Reliability and Timeliness in Payment-Related Matters)

1. The Garante shall encourage, pursuant to Section 12, adoption of a code of conduct and professional practice for the processing of personal data that is carried out within the framework of information systems owned by private entities, where they are used to grant consumer credits or else concern data subjects' reliability and timeliness in performing payments, by also laying down specific arrangements to facilitate communication of accurate, up-to-date personal data in compliance with data subjects' rights.

Section 118

(Commercial Information)

1. The Garante shall encourage, pursuant to Section 12, adoption of a code of conduct and professional practice for the processing of personal data that is carried out for commercial information purposes, by also setting forth simplified arrangements to inform data subjects and appropriate mechanisms to ensure quality and accuracy of the data collected and communicated, in line with the provisions made in Section 13(5).

Section 119

(Data Concerning Payment of Debts)

1. The code of conduct and professional practice referred to in Section 118 shall also lay down harmonised retention periods for the personal data contained, in particular, in data banks, registers and lists kept by public and private bodies with regard to payment of debts by data subjects in cases other than those regulated by the Code referred to in Section 117. Account shall have to be taken of the specific features of the processing operations carried out in the different sectors.

Section 120

(Car Accidents)

1. The Istituto per la vigilanza sulle assicurazioni private e di interesse collettivo (ISVAP) [Supervisory Body for Private Insurance] shall lay down procedural and operational mechanisms applying to the car accidents data bank that was set up to prevent and fight fraud in connection with the compulsory insurance for motor vehicles registered in Italy; further, the arrangements for accessing the information collected in said data bank as regards judicial authorities and public administrative agencies that are competent over prevention of and fight against fraud in the compulsory insurance sector as well as limitations on and arrangements for access to said information by insurance companies shall be set out.

2. Personal data may be processed and communicated to the entities referred to in paragraph 1 in order to discharge the tasks referred to in said paragraph.

3. [14] To the matters that are not regulated by this Section there shall apply the provisions contained in Section 135 of the Private Insurance Code.

TITLE X – ELECTRONIC COMMUNICATIONS

CHAPTER I – ELECTRONIC COMMUNICATION SERVICES

Section 121

(Services Concerned)

1. This Title shall apply to the processing of personal data in connection with the provision of publicly accessible electronic communication services on public communications networks.

[14] This paragraph was amended by Section 352 of the Private Insurance Code as per legislative decree no. 209 dated 7 September 2005; the amendment came into force as of 1 January 2006.

Section 122

(Information Collected with Regard to Subscribers or Users)

1. Subject to paragraph 2, it shall be prohibited to use an electronic communication network to gain access to information stored in the terminal equipment of a subscriber or user, to store information or monitor operations performed by an user.

2. The Code of conduct referred to in Section 133 shall lay down prerequisites and limitations for a provider of an electronic communication service to use the network in the manner described in paragraph 1 for specific, legitimate purposes related to technical storage for no longer than is strictly necessary to transmit a communication or provide a specific service as requested by a subscriber or user that has given his/her consent based on prior information as per Section 13, whereby purposes and duration of the processing shall have to be referred to in detail, clearly and accurately.

Section 123

(Traffic Data)

1. Traffic data relating to subscribers and users that are processed by the provider of a public communications network or publicly available electronic communications service shall be erased or made anonymous when they are no longer necessary for the purpose of transmitting the electronic communication, subject to paragraphs 2, 3 and 5.

2. Providers shall be allowed to process traffic data that are strictly necessary for subscriber billing and interconnection payments for a period not in excess of six months in order to provide evidence in case the bill is challenged or payment is to be pursued, subject to such additional retention as may be specifically necessary on account of a claim also lodged with judicial authorities.

3. For the purpose of marketing electronic communications services or for the provision of value added services, the provider of a publicly available electronic communications service may process the data referred to in paragraph 2 to the extent and for the duration necessary for such services or marketing, on condition that the subscriber or user to whom the data relate has given his/her consent. Such consent may be withdrawn at any time.

4. In providing the information referred to in Section 13, the service provider shall inform a subscriber or user on the nature of the traffic data processed as well as on duration of the processing for the purposes referred to in paragraphs 2 and 3.

5. Processing of traffic data shall be restricted to persons in charge of the processing who act – pursuant to Section 30 – directly under the authority of the provider of a publicly available electronic communications service or, where applicable, the provider of a public communications network and deal with billing or traffic management, customer enquiries, fraud detection, marketing of electronic communications or the provision of value-added services. Processing shall be restricted to what is absolutely necessary for the purposes of such activities and must allow identification of the person in charge of the processing who accesses the data, also by means of automated interrogation procedures.

6. The Authority for Communications Safeguards may obtain traffic and billing data that are necessary for settling disputes, particularly with regard to interconnection or billing matters.

Section 124

(Itemised Billing)

1. Subscribers shall have the right to receive, upon request and free of charge, detailed proof of the items making up the bill, in particular concerning date and starting time of a conversation, selected numbers, type of numbering, place, duration and units charged for each conversation.

2. The provider of a publicly available electronic communications service shall be required to enable users to perform communications and request services from any terminal equipment - free of charge and using simple means – by availing themselves of alternative payment methods, including anonymous methods, such as credit cards, debit cards or pre-paid cards.

3. The services and communications referred to in paragraph 2 and the communications required to implement alternative payment methods shall not be displayed in the documents sent to subscribers concerning the communications performed.

4. The final three digits of the called numbers shall not be displayed in subscriber bills. A subscriber may request communication of the full numbers relating to the communications at stake for the sole purpose of specifically challenging either the accuracy of certain charges or charges relating to limited periods.

5. Having established that the methods referred to in paragraph 2 are actually available, the Garante may authorise the provider to report the full numbers in the bills.

Section 125

(Calling Line Identification)

1. Where presentation of calling line identification is available, the provider of a publicly available electronic communications service shall ensure that the calling user has the possibility, free of charge and using simple means, to eliminate the presentation of calling line identification on a per-call basis. The calling subscriber must have the same possibility on a per-line basis.

2. Where presentation of calling line identification is available, the provider of a publicly available electronic communications service shall ensure that the called subscriber has the possibility, free of charge and using simple means, to prevent presentation of identification of incoming calls.

3. Where presentation of calling line identification is available and such identification is presented prior to the call being established, the provider of a publicly available electronic communications service shall ensure that the called subscriber has the possibility, free of charge and using simple means, to reject incoming calls if the presentation of calling line identification has been eliminated by the calling user or subscriber.

4. Where presentation of connected line identification is available, the provider of a publicly available electronic communications service shall ensure that the called subscriber has the possibility, free of charge and using simple means, to prevent the presentation of connected line identification to the calling user.

5. Paragraph 1 shall also apply to calls to countries outside the European Union. Paragraphs 2 to 4 shall also apply with regard to calls originating in said countries.

6. Where presentation of calling or connected line identification is available, the provider of a publicly available electronic communications service shall inform subscribers and users of the existence of such service as well as of the possibilities referred to in paragraphs 1, 2, 3 and 4.

Section 126

(Location Data)

1. Location data other than traffic data, relating to users or subscribers of public communications networks or publicly available electronic communications services, may only be processed when they are made anonymous, or with the prior consent of the users or subscribers, which may be withdrawn at any time, to the extent and for the duration necessary for the provision of a value added service.

2. The service provider must inform the users or subscribers, prior to obtaining their consent, of the type of location data other than traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service.

3. Where consent of the users or subscribers has been obtained for the processing of location data other than traffic data, the user or subscriber shall continue to have the possibility, using a simple means and free of charge, of requesting to temporarily refuse the processing of such data for each connection to the network or for each transmission of a communication.

4. Processing of location data other than traffic data in accordance with paragraphs 1, 2 and 3 shall be restricted to persons in charge of the processing acting pursuant to Section 30 under the authority of the provider of the publicly available communications service or, as the case may be, the public communications network or of the third party providing the value added service. Processing shall be restricted to what is necessary for the purposes of providing the value added service and must ensure identification of the persons in charge of the processing that access the data also by means of automated interrogation operations.

Section 127

(Nuisance and Emergency Calls)

1. Any subscriber receiving nuisance calls may request that the provider of a public communications network or publicly available electronic communications service override, on a

temporary basis, the elimination of the presentation of calling line identification and store the data concerning the origin of the incoming call. Overriding the elimination of the presentation of calling line identification may only be provided for in connection with the time ranges during which the nuisance calls take place and for no longer than fifteen days.

2. The request made in writing by the subscriber shall specify the manner in which the nuisance calls are received and, if it is preceded by a request made by phone, shall be forwarded within the following forty-eight hours.

3. The data stored pursuant to paragraph 1 may be communicated to a subscriber where the latter declares that he/she will only use them to protect himself/herself against nuisance calls. As for the services referred to in paragraph 1, the provider shall make available transparent procedures to subscribers and may charge them amounts not exceeding the costs actually incurred.

4. The provider of a public communications network or publicly available electronic communications service shall set out transparent procedures in order to ensure that the services authorised to deal with emergency calls may override, on a per-line basis, the elimination of the presentation of calling line identification and, if necessary, process location data notwithstanding the temporary denial or absence of consent of the subscriber or user. Said services shall be specified in a decree issued by the Minister of Communications after seeking the opinion of the Garante and the Authority for Communications Safeguards.

Section 128

(Automatic Call Forwarding)

1. The provider of a publicly available electronic communications service shall take the measures required to allow each subscriber, free of charge and using simple means, to stop automatic call forwarding by third parties to his/her own terminal.

Section 129

(Directories of Subscribers)

1. The Garante shall issue a provision, in co-operation with the Authority for Communications Safeguards as per Section 154(3) as well as in compliance with Community legislation, to set out the arrangements for entering and subsequently using subscribers' personal data as contained in publicly available paper or electronic directories, also with regard to the data collected prior to entry into force of this Code.

2. The provision referred to in Section 1 shall lay down appropriate mechanisms for subscribers to give their consent to inclusion in said directories as well as to the use of their data for the purposes referred to in Section 7(4), letter b), the relevant principles consisting in the highest possible simplification of the mechanisms for being included in a directory that is only intended to allow searching the contact details of a subscriber, in the need for the subscriber's express, specific consent if the purposes of the processing are broader in scope as well as in the possibility for subscribers to access, rectify or erase their data free of charge.

Section 130

(Unsolicited Communications)

1. The use of automated calling systems without human intervention for the purposes of direct marketing or sending advertising materials, or else for carrying out market surveys or interactive business communication shall only be allowed with the user's consent.

2. Paragraph 1 shall also apply to electronic communications performed by e-mail, facsimile, MMS- or SMS-type messages or other means for the purposes referred to therein.

3. Except as provided for in paragraphs 1 and 2, further communications for the purposes referred to therein as performed by different means shall be allowed in pursuance of Sections 23 and 24 as well as under the terms of paragraph 3-bis below[15].

3-bis. By way of derogation from Section 129, processing by telephone and mail of the data referred to in Section 129(1) for the purposes set forth in Section 7(4), letter b., shall be allowed in respect of any entities that have not exercised their right to object, via simplified mechanisms including the use of electronic networks, by having the respective telephone numbers and other personal data as per Section 129(1) entered in a public opt-out register.[16] [Amended by Section 6(2)a, item 6. of decree no. 70 dated 13 May 2011]

3-ter. The register as per paragraph 3-bis shall be set up by a decree of the President of the Republic to be adopted in pursuance of section 17(2) of Act no. 400 dated 23 August 1988 following a resolution by the Council of Ministers, after obtaining the opinions of the Council of State and the competent Parliamentary Committees – to be rendered within thirty days of the respective requests – as well as the opinion of the Authority for Communications Safeguards with regard to the issues falling under the latter Authority's scope of competence – to be rendered within the same deadline; the following general standards and principles shall have to be followed:
a. the register shall be set up with and managed by a public body and/or organization that has vested competences in this area;
b. the body and/or organisation in charge for setting up and managing the register shall have to rely on the human resources and tools it holds at its disposal; alternatively, setting up and management

---

[15] This paragraph was amended by Section 20-bis, paragraph 1, letter a., of the decree no. 135 dated 25 September 2009, as converted with amendments into Act no. 166 dated 20 November 2009.

[16] This paragraph along with paragraph 3-ter and paragraph 3-quater was added by Section 20-bis, paragraph 1, letter b., of the decree no. 135 dated 25 September 2009, as converted with amendments into Act no. 166 dated 20 November 2009.
For the sake of completeness, paragraphs 2 to 4 of Section 20-bis of the aforementioned decree are reported below:
"2. The register mentioned in Section 130(3-bis) of the [Data Protection Code], as introduced by paragraph 1, letter b., of this section, shall be set up within six months as from the date of entry into force of [this] Act. Pending the said entry into force, the provisions adopted by the Italian data protection authority in pursuance of section 154 of the Data Protection Code, as subsequently amended, shall continue to be applicable in pursuance of section 129 thereof.
3. In section 44(1-bis) of decree no. 207 dated 30 December 2008 as converted, with amendments, into Act no. 14 dated 27 February 2009, the words "until 31 December 2009" shall be replaced by the following: "until expiry of a six-month period following the date of entry into force of the Act converting decree no. 135 dated 25 September 2009".
4. In section 58 of the Consumer Code as per legislative decree no. 206 dated 6 September 2005, paragraph 1 shall be replaced by the following: "1. Use by a professional of telephone, electronic mail, non-operator assisted automated calling systems, and/or facsimile shall require the consumer's prior consent - subject to the provisions contained in section 130(3-bis) of the personal data protection Code (legislative decree no. 196/2003) – as for processing of the data contained in publicly available subscriber directories."

of the register may be committed to third parties, which shall undertake to be liable for all the relevant financial and organisational charges, by way of a contract for the supply of services in accordance with the Code of Public Contracts relating to works, services and supplies as per legislative decree no. 163 dated 12 April 2006. The entities resorting to the register in order to carry out their communications shall be charged an access tariff based on the actual operational and maintenance costs. The Ministry for Economic Development shall determine the said tariffs by an order;
c. The technical arrangements applying to operation of the register shall be such as to enable every user to request that the respective number be entered in the register via simplified mechanisms including the use of electronic networks and/or the telephone;
d. The technical arrangements applying to operation of and access to the register shall be such as to enable selective queries that should not allow transferring the data contained in the said register, whereby all the operations shall be logged and the access data shall be stored;
e. The timeline and arrangements for entering and updating information in the register shall be set forth, whereby no distinction shall be drawn in terms of industry sector and/or type of commodity, and the maximum period shall be laid down during which the validated data contained in the register may be used; it shall be provided that the data are entered in the register for an indefinite amount of time and may be removed therefrom at any time via simple mechanisms and free of whatever charge;
f. any entities processing data for the purposes mentioned in section 7(4), letter b., shall be required to ensure presentation of calling line identification and provide the appropriate information to users, with particular regard to the possibility and arrangements to have their data entered in the register so as to object to being contacted in future;
g. it shall be provided that inclusion in the register does not prevent processing of the data that have been acquired via other channels and are processed in compliance with sections 23 and 24.

3-quater. Supervision and control over organisation and operation of the register as per paragraph 3-bis and the relevant data processing operations shall be committed to the Italian data protection authority.

4. Subject to paragraph 1, where a data controller uses, for direct marketing of his/her own products or services, electronic contact details for electronic mail supplied by a data subject in the context of the sale of a product or service, said data controller may fail to request the data subject’s consent, on condition that the services are similar to those that have been the subject of the sale and the data subject, after being adequately informed, does not object to said use either initially or in connection with subsequent communications. The data subject shall be informed of the possibility to object to the processing at any time, using simple means and free of charge, both at the time of collecting the data and when sending any communications for the purposes referred to in this paragraph.

5. In any event, the practice of sending communications for the purposes referred to in paragraph 1 or anyhow for promotional purposes by disguising or concealing the identity of the sender, or without a valid address to which the data subject may send a request to exercise the rights referred to in Section 7, shall be prohibited.

6. In case of persistent breach of the provisions laid down in this Section, the Garante may also order the provider of electronic communications services, under Section 143(1), letter b), to implement filtering procedures or other practicable measures with regard to the electronic contact details for electronic mail used for sending the communications.

Section 131

(Information Provided to Subscribers and Users)

1. The provider of a publicly available electronic communications service shall inform subscribers and, if possible, users concerning the existence of situations that allow the contents of communications or conversations to be unintentionally made known to persons who are not party to them.

2. Subscribers shall inform users whenever the contents of communications or conversations may come to be known by others either because of the type of terminal equipment used or because of the connection established between such terminal equipment at the subscribers' premises.

3. An user shall inform another user whenever, during a conversation, devices are used to enable said conversation to be heard by others.

Section 132[17]

(Traffic Data Retention for Other Purposes)

1. [18] Without prejudice to Section 123(2), telephone traffic data shall be retained by the provider for twenty-four months as from the date of the communication with a view to detecting and suppressing criminal offences, whereas electronic communications traffic data, except for the contents of communications, shall be retained by the provider for twelve months as from the date of the communication with a view to the same purposes.

1-bis. The data related to unsuccessful calls that are processed on a provisional basis by the providers of publicly available electronic communications services or a public communications network shall be retained for thirty days.[19]

2. [20] [Repealed.]

3. Within the term referred to in paragraph 1, the data may be acquired from the provider by means of a reasoned order issued by the public prosecutor also at the request of defence counsel, the person under investigation, the injured party, or any other private party. Defence counsel for either

---

[17] As amended by Decree-Law no. 354 of 24th December 2003, converted, with amendments, into Act no. 45 of 26th February 2004; Decree-Law no. 144 of July 27, 2005 converted with amendments into Act no. 155 of July 31, 2005 ("Urgent Measures to Fight Terrorism"), Decree-Law no. 248/2007 converted with amendments into Act no. 31/2008 dated 27 February 2008, Act no. 48 dated 18 March 2008 ratifying the Council of Europe's Convention on Cybercrime of 23 November 2001, and Presidential Decree no. 109 dated 30 May 2008 (implementing directive 2006/24/EC).
An excerpt of the relevant provisions contained in the decree-law no. 144/2005 is reported here for the sake of completeness, as subsequently amended by decree no. 248 dated 31 December 2007 converted with amendments into Act no. 31/2008 dated 27 February 2008:
"Article 6. (*New Provisions on Telephone and Internet Traffic Data*) (1) As of the date of entry into force of this decree [August 2, 2005] until entry into force of the legislative instrument implementing directive 2006/24/EC of the European Parliament and the Council, of 15 March 2006, and in any case until no later than 31 December 2008, application of laws, regulations and/or administrative measures providing and/or allowing for erasure of telephone and/or electronic communications traffic data shall be suspended, regardless of whether the said data are needed for billing purposes; the data in question shall have to be retained by providers of publicly available communications networks and/or electronic communications services until entry into force of the legislative instrument implementing directive 2006/24/EC of the European Parliament and the Council, of 15 March 2006, and in any case until no later than 31 December 2008, except for the contents of the communications and by having regard to the information allowing accesses and – where available – services to be tracked, whereby any provisions in force envisaging longer retention periods shall have to be left unprejudiced. Any traffic data that is retained beyond the period set out in Section 132 of legislative decree no. 196/2003 may only be used for the purposes set out herein, subject to prosecution of offences that are prosecutable in any case.
(…)
Article 7. (*Provisions Supplementing the Administrative Measures on Public Establishments Offering Telephone and Internet Access Points*). (1). As of the fifteenth day following the date of entry into force of this decree [August 2, 2005] until December 31, 2008, whoever plans to open up a public establishment and/or a private club of whatever kind whose activity consists, either exclusively or predominantly, in making available terminal equipment to the public, customers and/or members, whereby the said equipment may be used for electronic or other communications, or where over three pieces of such equipment are installed, shall have to apply to the competent *questore* [Head of provincial police office] for a licence. No licence shall be required if only public payphones are installed allowing exclusively voice calls to be made.
(2) As regards the entities already carrying out the activities referred to in paragraph 1, the licence shall have to be applied for within sixty days as of the date of entry into force of this decree."

[18] This paragraph was amended firstly by Section 6(3) of decree no. 144/2005, and thereafter by Section 2 of legislative decree no. 109/2008.

[19] This paragraph was added by Section 2 of legislative decree no. 109/2008 and entered into force as per the time schedule set forth in Section 6(3) thereof.

[20] This paragraph was repealed by Section 2(1)c. of legislative decree no. 109/2008 along with paragraph 4 and paragraph 4-bis hereof..

the defendant or the person under investigation may directly request the provider to make available the data relating to the subscriptions entered into by his/her client according to the arrangements specified in Section 391-quater of the Criminal Procedure Code without prejudice to the requirements set out in Section 8(2), letter f), with regard to incoming phone calls.

4. [Repealed.]

4-bis. [Repealed.]

4-ter.[21] The Minister for Home Affairs or the heads of the central offices specialising in computer and/or IT matters from the State Police, the Carabinieri, and the Financial Police as well as the other entities mentioned in paragraph 1 of section 226 of the implementing, consolidating, and transitional provisions related to the Criminal Procedure Code as per legislative decree no. 271/1989, where delegated by the Minister for Home Affairs, may order IT and/or Internet service providers and operators to retain and protect Internet traffic data, except for contents data, according to the arrangements specified above and for no longer than ninety days, also in connection with requests lodged by foreign investigating authorities, in order to carry out the pre-trial investigations referred to in the said section 226 of the provisions enacted via legislative decree no. 271/1989, or else with a view to the detection and suppression of specific offences. The term referred to in the order in question may be extended, on grounds to be justified, up to six months whilst specific arrangements may be made for keeping the data as well as for ensuring that the data in question are not available to the IT and/or Internet service providers and operators and/or to third parties.

4-quater. Any IT and/or Internet service providers and/or operators that are the subject of the order mentioned in paragraph 4-ter shall comply without delay and forthwith give assurances to the requesting authority as to their compliance. IT and/or Internet service providers and/or operators are required to keep the order at issue confidential along with any activities performed accordingly throughout the period specified by the said authority. Violation of this requirement shall be punished in accordance with section 326 of the Criminal code unless the facts at issue amount to a more serious offence.

4-quinquies. The measures taken under paragraph 4-ter above shall be notified in writing without delay, in any case by forty-eight hours as from service on the addressee(s), to the public prosecutor that is competent for the place of enforcement, who shall endorse them if the relevant preconditions are fulfilled. The measures shall cease to be enforceable if they are not endorsed.

5. [22] Data processing for the purposes referred to in paragraph 1 shall be carried out by complying with the measures and precautions to safeguard data subjects as required under Section 17, which are aimed at ensuring that the retained data fulfil the same quality, security and protection requirements as network data as well as at:

a. providing in all cases for specific systems allowing both computer-based authentication and authorisation of persons in charge of the processing as per Annex B,
b.[23] [Repealed.]
c. [Repealed.]
d. [24] laying down technical mechanisms to regularly destroy the data after expiry of the term referred to in paragraph 1.

---

[21] This paragraph was added by Section 10 of Act no. 48 dated 10 March 2008 along with paragraph 4-quater and 4-quinquies hereof.
[22] This paragraph was amended by Section 2(1)d. of legislative decree no. 109/2008.
[23] This letter was repealed by Section 2(1)d. of legislative decree no. 109/2008 along with letter c. hereof.

CHAPTER II – INTERNET AND ELECTRONIC NETWORKS

Section 133

(Code of Conduct and Professional Practice)

1. The Garante shall encourage, pursuant to Section 12, adoption of a code of conduct and professional practice applying to the processing of personal data by providers of communication and information services supplied by means of electronic communications networks, with particular regard to the criteria to ensure and streamline adequate information and awareness by users of public and private electronic communications networks as to the categories of personal data processed and the mechanisms for such processing – in particular, by providing information notices online using simple means and in an interactive manner, so as to enhance openness and fairness in respect of the users as well as full compliance with the principles referred to in Section 11 also with a view to certifying quality of the implemented mechanisms and the security level afforded.

CHAPTER III – VIDEO SURVEILLANCE

Section 134

(Code of Conduct and Professional Practice)

1. The Garante shall encourage, pursuant to Section 12, adoption of a code of conduct and professional practice applying to the processing of personal data that is performed by means of electronic image acquisition devices, by setting forth specific processing arrangements and simplified mechanisms to inform data subjects in order to ensure lawfulness and fairness of the processing also in the light of Section 11.

TITLE XI – SELF-EMPLOYED PROFESSIONALS AND PRIVATE DETECTIVES

CHAPTER I – IN GENERAL

Section 135

(Code of Conduct and Professional Practice)

1. The Garante shall encourage, pursuant to Section 12, adoption of a code of conduct and professional practice applying to the processing of personal data that is performed to carry out investigations by defence counsel as per Act no. 397 of 7 December 2000 or else to establish or

[24] This letter was amended by Section 2(1)d., point 3, of legislative decree no. 109/2008.

defend a legal claim, in particular as regards self-employed professionals and entities authorised under the law to operate as private detectives.

TITLE XII – JOURNALISM AND LITERARY AND ARTISTIC EXPRESSION

CHAPTER I – IN GENERAL

Section 136

(Journalistic Purposes and Other Intellectual Works)

1. This Title shall apply to processing operations

a) that are carried out in the exercise of the journalistic profession and for the sole purposes related thereto;

b) that are carried out by persons included either in the list of free-lance journalists or in the roll of trainee journalists as per Sections 26 and 33 of Act no. 69 of 03.02.63;

c) that are carried out on a temporary basis exclusively for the purposes of publication or occasional circulation of articles, essays and other intellectual works also in terms of artistic expression.

Section 137

(Applicable Provisions)

1. The provisions laid down in this Code concerning

a) the authorisation granted by the Garante pursuant to Section 26,

b) the safeguards referred to in Section 27 in connection with judicial data,

c) cross-border data flows as per Title VII of Part I,

shall not apply to the processing operations referred to in Section 136.

2. The data processing operations referred to in paragraph 1 may be performed also in the absence of the data subject’s consent as per Sections 23 and 26.

3. If the data are communicated or disseminated for the purposes referred to in Section 136, the limitations imposed on freedom of the press to protect the rights as per Section 2, in particular concerning materiality of the information with regard to facts of public interest, shall be left

unprejudiced. It shall be allowed to process the data concerning circumstances or events that have been made known either directly by the data subject or on account of the latter's public conduct.

Section 138

(Professional Secrecy)

1. The provisions concerning professional secrecy in the journalistic profession shall be left unprejudiced as related to the source of the information if a data subject requests to be informed of the source of the personal data in accordance with Section 7(2), letter a).

CHAPTER II – CODE OF PRACTICE

Section 139

(Code of Practice Applying to Journalistic Activities)

1. The Garante shall encourage, pursuant to Section 12, adoption of a code of practice by the National Council of the Press Association as regards processing of the data referred to in Section 136. The code shall include measures and provisions to safeguard data subjects as appropriate in respect of the nature of the data, with particular regard to those disclosing health and sex life. The code may also lay down simplified arrangements for providing the information referred to in Section 13.

2. In the course of drawing up said code, or thereafter, the Garante in cooperation with the Council shall lay down measures and provisions to safeguard data subjects, which the Council shall have to adopt.

3. Where the code of practice or any amendments or additions thereto fail to be adopted by the Council within six months of the proposal put forward by the Garante, they shall be adopted vicariously by the Garante and enforced until different regulations come into force pursuant to the cooperation procedure.

4. The code and any amendments or additions thereto shall come into force fifteen days after publication in the Official Journal as per Section 12.

5. Should any of the provisions in the code of practice be infringed, the Garante may prohibit the processing pursuant to Section 143(1), letter c).

TITLE XIII – DIRECT MARKETING

CHAPTER I – IN GENERAL

Section 140

(Code of Conduct and Professional Practice)

1. The Garante shall encourage, pursuant to Section 12, adoption of a code of conduct and professional practice applying to the processing of personal data that is performed to send advertising materials or for direct selling purposes, or else to carry out market surveys or commercial communication activities, by also laying down simplified arrangements for a data subject to indicate and highlight his/her objection to receiving certain communications whenever the data subject's consent is not a prerequisite for the processing.

PART III – REMEDIES AND SANCTIONS

TITLE I – ADMINISTRATIVE AND JUDICIAL REMEDIES

CHAPTER I – REMEDIES AVAILABLE TO DATA SUBJECTS BEFORE THE GARANTE

I – GENERAL PRINCIPLES

Section 141

(Available Remedies)

1. Data subjects may apply to the Garante

a) to lodge a circumstantial claim pursuant to Section 142, in order to point out an infringement of the relevant provisions on the processing of personal data,

b) to lodge a report, if no circumstantial claim as per letter a) may be lodged, in order to call upon the Garante to check up on the aforementioned provisions,

c) to lodge a complaint with a view to establishing the specific rights referred to in Section 7 in accordance with the arrangements and for the purposes laid down in Part III of this Chapter.

II – ADMINISTRATIVE REMEDIES

Section 142

(Lodging a Claim)

1. A claim shall refer, with as many details as possible, to the facts and circumstances on which it is grounded, the allegedly infringed provisions and the remedies sought as well as to the identification data concerning data controller, data processor, if available, and claimant.

2. The claim shall be undersigned either by the data subjects or by associations representing them also pursuant to Section 9(2) and shall be lodged with the Garante without any specific formalities being required. Such documents as may be helpful for assessment purposes shall be annexed to the claim including the relevant letter of attorney, if any, and an address shall be specified to send communications also by e-mail, facsimile or telephone.

3. The Garante may draw up a claim form to be published in the Bulletin and made available via electronic means.

Section 143

(Handling a Claim)

1. Upon conclusion of the preparatory phase, if the claim is not found to be manifestly groundless and the prerequisites for a decision are fulfilled, the Garante

a) may call upon the data controller – also requesting the latter to appear jointly with the data subject – to autonomously block the processing before ordering that the measures referred to in letter b) are taken, or before prohibiting or blocking the processing as per letter c),

b) shall order that the data controller takes such measures as are necessary or appropriate to bring the processing into line with the provisions in force,

c) shall block or prohibit the processing, in whole or in part, if the latter is found to be unlawful or unfair partly because of the failure to take the necessary measures as per letter b), or else if there is an actual risk that it may be considerably prejudicial to one or more of the data subjects by having regard to the nature of the data, the arrangements applying to the processing or the effects that may be produced by the processing,

d) may prohibit, in whole or in part, processing of data concerning individual entities or categories if it is in conflict with the substantial public interest,

also prior to finalising the relevant proceeding.

2. The provisions referred to in paragraph 1 shall be published in the Official Journal of the Italian Republic if the relevant addressees cannot be easily identified on account either of their number or of the complexity of the inquiries.

Section 144

(Reports)

1. The provisions referred to in Section 143 may also be taken in connection with a report lodged as per Section 141(1), letter b), if preliminary investigations have already been started, also prior to finalising the relevant proceeding.

III – NON-JUDICIAL REMEDIES

Section 145

(Complaints)

1. The rights as per Section 7 may be enforced either by filing a lawsuit or by lodging a complaint with the Garante.

2. Lodging a complaint with the Garante shall not be permitted if an action regarding the same matter and between the same parties has already been brought before a judicial authority.

3. Lodging a complaint with the Garante shall prevent an action from being brought by the same parties and for the same matter before a judicial authority.

Section 146

(Prior Request to Data Controller or Processor)

1. Except where the running of time would cause imminent, irreparable harm to a person, lodging a complaint with the Garante shall only be permitted after a request concerning the same matter has been made to the data controller or processor pursuant to Section 8(1) and the term provided for in this Section has expired, or else if said request has not been granted also in part.

2. A response to the request shall be provided by the data controller or processor within fifteen days of its receipt.

3. Within the deadline referred to in paragraph 2, the data controller or processor shall inform the data subject that the operations required to fully comply with his/her request are especially complex, or that delay can be accounted for on other grounds. In this case, the request shall have to be complied with in full within thirty days of its receipt.

Section 147

(Lodging a Complaint)

1. A complaint shall be lodged against the data controller by specifying:

a) name of complainant, special agent, if any, data controller and, where known, the data processor that has been designated to provide responses to data subjects exercising the rights referred to in Section 7;
b) date of the request made to the data controller or processor pursuant to Section 8(1), or else the imminent, irreparable harm making said request unnecessary;
c) the grounds for the complaint;
d) the remedy sought from the Garante;
e) the domicile of choice for the purposes of the relevant proceeding.

2. The complaint shall be undersigned by either the complainant or the latter’s special agent and include as attachments

a) a copy of the request made to the data controller or processor pursuant to Section 8(1);
b) the letter of attorney, if any;
c) proof of the payment of office charges.

3. Any documents that may be helpful in evaluating the complaint shall be also attached, including an address for the service of communications on either the complainant or the special agent by e-mail, facsimile or telephone.

4. The complaint shall be lodged with the Garante and the relevant signature shall be certified true. No certification shall be necessary if the complaint is undersigned either at the Office of the Garante or by a special agent who is included in the roll of lawyers and has been granted power of attorney in accordance with Section 83 of the Civil Procedure Code, or else if it is electronically signed pursuant to the legislation in force.

5. Complaints shall have to be lodged exclusively either by registered letter or by electronic networks in compliance with the arrangements concerning digital signature and receipt confirmation that are referred to in Section 38(2); alternatively, they may be lodged directly with the Office of the Garante.

Section 148

(Inadmissible Complaints)

1. A complaint shall be inadmissible

a) if it is lodged by a person having no legitimate title thereto,

b) if Sections 145 and 146 are not complied with,

c) in default of any of the items referred to in Section 147(1) and (2), unless the complainant or the special agent amend the complaint, also following the invitation made by the Office of the Garante in accordance with paragraph 2, within seven days of the date on which it was lodged or said invitation was received. In this case, the complaint shall be regarded as lodged at the time when the amended complaint is received by the Office.

2. The Garante shall specify the cases in which a complaint may be amended.

Section 149

(Handling a Complaint)

1. The Office of the Garante shall be responsible for communicating a complaint to the data controller within three days, except where it has been declared to be inadmissible or manifestly groundless, also informing said controller that he/she may notify both the complainant and the Office within ten days of the receipt of the above communication that he/she will voluntarily comply. Said information shall be provided to the data controller by the data processor, if any, that has been designated to provide responses to data subjects in case the rights as per Section 7 are exercised, on condition that this is referred to in the complaint.

2. In case of voluntary compliance, a declaration of no case to answer shall be returned. Upon the complainant’s request, costs and charges relating to the complaint shall be calculated as a lump sum and either awarded to the opposing party or balanced, also in part, on rightful grounds.

3. The data controller, the data processor referred to in paragraph 1 and the data subject shall have the right of being heard, whether personally or through a special agent, and of submitting pleadings or documents. To that end, the communication referred to in para. 1 shall be also sent to the complainant and specify the term within which the data controller, processor or data subject may submit pleadings and documents as well as the day on which said persons may be heard, also by means of suitable audiovisual techniques.

4. In the course of the proceeding, the complainant may better specify his/her claim to the extent that it falls within the scope of the complaint, or else if the data controller raises objections.

5. The Garante may order, also ex officio, that one or more expert assessments be carried out. The relevant order shall specify the scope of such assessment and its deadline and shall be communicated to the parties, who may attend either personally or through their agents or advisors. The order shall also make arrangements for the payment in advance of any costs relating to the assessment.

6. The data controller and the data processor referred to in paragraph 1 may be assisted in the proceeding by an agent or a person of their choice.

7. If the enquiries are especially complex or the parties agree thereto, the sixty-day term referred to in Section 150(2) may be extended by no more than forty additional days.

8. Running of time as per Section 150(2) and Section 151 shall be stopped by operation of law from 1 August to 15 September of each year and shall start again as of the end of the latter period. Should time start running during said period, the start shall be postponed to the end of the selfsame period. Running of time shall not be stopped whenever there exists the harm referred to in Section 146(1) and its stopping shall not prevent taking the measures referred to in Section 150(1).

Section 150

(Measures Taken Following a Complaint)

1. If so required by the specific case, the Garante may provisionally order either the partial or total blocking of some of the data, or the immediate termination of one or more processing operations. Such order may also be adopted prior to communicating the complaint as per Section 149(1) and shall cease to be effective if the decision mentioned in paragraph 2 is not rendered within the relevant deadline. The order may be challenged together with said decision.

2. Having gathered the necessary information, the Garante shall order with a reasoned decision, if the complaint is found to be grounded, that the data controller abstain from the unlawful conduct; the Garante shall also specify the remedies to enforce the data subject’s rights and set a term for their implementation. If no decision on the complaint is rendered within sixty days of the date on which the complaint was lodged, the complaint shall have to be regarded as dismissed.

3. If any party previously requested it, the provision by which the proceeding is finalised shall also set out the costs and office charges relating to the complaint as a lump sum either to be awarded, also in part, to the losing party, or to be compensated for, also in part, on rightful grounds.

4. The decision taken by the Garante, regardless of its being provisional, shall be communicated to the parties within ten days either at their domiciles of choice or at the domiciles specified in the case records. Said decision may be communicated to the parties also by e-mail or facsimile.

5. If enforcement of the decision referred to in paragraphs 1 and 2 proves difficult or is objected to, the Garante shall lay down implementing arrangements, after hearing the parties if appropriate, by availing itself, if necessary, either of Office staff or of the collaboration of other public authorities.

6. If the provision in which costs and charges are set out is not challenged, or if it is dismissed, said provision shall be regarded as an enforcement order pursuant to Sections 474 and 475 of the Civil Procedure Code with regard to such costs and charges.

Section 151

(Challenging)

1. The decision and/or tacit dismissal referred to in Section 150(2) may be challenged by the data controller or the data subject, as the case may be, in that they may file a petition pursuant to Section 152. Challenging shall not suspend enforcement of the decision.

2. Courts shall follow the procedure set out in Section 152.

CHAPTER II – JUDICIAL REMEDIES

Section 152

(Judicial Authorities)

1. Competence over any disputes concerning application of the provisions of this Code, including those related either to provisions issued by the Garante with regard to personal data protection or to the failure to adopt such provisions, shall lie with judicial authorities.

2. As regards any dispute referred to in paragraph 1, the relevant proceeding shall be instituted by filing a petition with the clerk’s office of the court having jurisdiction on the data controller’s place of residence.

3. The judicial authority shall decide on the case as a single-judge court.

4. Any petition against a provision by the Garante, also in pursuance of Section 143, shall have to be filed within thirty days of the date on which said provision is communicated or tacitly dismissed. If the petition is filed thereafter, the court shall declare that it is inadmissible by an order that may be challenged before the Court of Cassation.

5. Filing of a petition shall not suspend enforcement of the provision by the Garante. The court may provide wholly or partly otherwise on serious grounds, after hearing the parties, by issuing an order that may be challenged together with the decision finalising the relevant proceeding.

6. If there is an imminent danger of serious, irretrievable harm, the court may take the necessary measures by a reasoned decree, also summoning the parties to appear in court by no later than fifteen days. During the relevant hearing the court shall uphold, amend or discharge the measures taken by means of said decree.

7. The court shall summon the parties to appear by a decree in which the petitioner shall be notified of the mandatory term within which he/she shall have to serve said decree on the other parties as well as on the Garante. There shall be an interval of no less than thirty days between the day of service and the day in court.

8. Should the petitioner fail to appear on the first day in court without alleging any lawful grounds, the court shall order that the case be struck off the cause list and declare that the relevant proceeding is expired, also awarding costs to the petitioner.

9. When dealing with the case, the court shall decide on the items of evidence that it deems to be necessary, also of its own motion and without any formalities that are unnecessary for dealing with the case in court, and may order that witnesses be summoned also without laying down the relevant chapters.

10. Upon completion of the preparatory phase, the court shall invite the parties to sum up their cases and proceed with the oral argument. The court shall issue a judgment immediately thereafter by reading the relevant instrument. The reasons for the judgment shall be deposited with the court's clerk's office in the next thirty days. The court may also draw up and read the reasons jointly with the formal judgment, both being deposited with the court's clerk's office immediately thereafter.

11. If necessary, the court may grant no more than ten days for the parties to submit pleadings and adjourn to the first useful day following expiry of the above term with a view to the oral argument and issuing of the judgment.

12. With its judgment, the court shall grant or dismiss the petition, in whole or in part, order the necessary measures, provide for damages, if claimed, and award legal costs to the losing party, also by derogating from the prohibition referred to in Section 4 of Act no. 2248 of 20 March 1865, Annex E), whenever this is necessary in connection with, inter alia, acts performed by a public body in its capacity as data controller or processor.

13. The judgment may not be appealed against, however it may be challenged before the Court of Cassation.

14. This Section shall also apply to the cases referred to in Section 10(5) of Act no. 121 of 1 April 1981 as subsequently amended.

TITLE II – THE SUPERVISORY AUTHORITY

CHAPTER I – THE GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Section 153

(The Garante)

1. The Garante shall act fully autonomously and independently in its decisions and assessments.

2. The Garante shall be a collegiate body composed of four members, of whom two shall be elected by the Chamber of Deputies and two by the Senate through a specific voting procedure. The members shall be persons ensuring independence and with proven experience in the field of law or computer science; experts from both sectors shall have to be included.

3. The members shall elect their President, who shall have the casting vote in the case where votes are equal. They shall also elect a Vice-President, who shall discharge the functions of the President if the latter is absent or hindered.

4.[25] President and members shall hold office for seven years; their appointment shall not be renewable. For the entire term of their office, President and members shall not be allowed - under penalty of losing office - to carry out professional or advisory activities, manage or be employed by public or private entities or hold elective offices.

5. Once President and members have accepted their appointment, they shall be assigned to the temporary staff if they are employees in the public administration or judges/prosecutors not yet retired; if they are faculty professors at an University, they shall be put on leave of absence with no allowances pursuant to Section 13 of Presidential decree no. 382 of 11.07.1980 as subsequently amended. Staff who have been assigned to the temporary staff or put on leave of absence may not be replaced.

6. The President shall be entitled to an allowance not exceeding the one paid to the judge presiding over the Court of Cassation (*Corte di Cassazione*). Members shall be entitled to an allowance not exceeding two-thirds of that paid to the President. The aforementioned allowances shall be determined pursuant to Section 6 of Presidential Decree no. 501 of 31 March 1998 in such a way as to be included in the ordinary budget.

7. The Office referred to in Section 156 shall be under the authority of the Garante.

[25] This paragraph was amended by section 47-quater of Act no. 31/2008, which brought about amendments to the term of office of the commissioners appointed to certain independent authorities (seven years) including the members making up the Italian data protection authority. The previous term of office was four years and was renewable once.

Section 154

(Tasks)

1. Notwithstanding specific provisions, the tasks to be discharged by the Garante, also with the help of the Office and in compliance with this Code, shall consist in:

a) verifying whether data processing operations are carried out in compliance with laws and regulations in force as well as with the relevant notification, also in case of termination of processing operations and with regard to the retention of traffic data[26];

b) receiving reports and complaints, and taking steps as appropriate with regard to the complaints lodged by other data subjects or the associations representing them;

c) ordering data controllers or processors, also ex officio, to adopt such measures as are necessary or appropriate for the processing to comply with the provisions in force as per Section 143;

d) prohibiting, also ex officio, unlawful or unfair data processing operations, in whole or in part, or blocking such processing operations pursuant to Section 143, and taking other measures as provided for by the legislation applying to processing of personal data;

e) encouraging the adoption of codes pursuant to Section 12 and Section 139;

f) drawing the attention of Parliament and Government to the advisability of legislation as required by the need to protect the rights referred to in Section 2, also in the light of sectoral developments;

g) giving opinions whenever required;

h) raising public awareness of the legislation applying to personal data processing and the relevant purposes as well as of the data security measures;

i) preferring information on facts and/or circumstances amounting to offences to be prosecuted ex officio, which it has come to know either in discharging or on account of its duties;

l) keeping the register of processing operations as drawn up on the basis of the notifications referred to in Section 37;

m) drawing up an annual report on the activity performed and implementation of this Code, which shall be submitted to Parliament and the Government by 30 April of the year following that to which the report refers.

2. Pursuant to paragraph 1, the Garante shall also discharge supervisory or assistance tasks concerning personal data processing as provided for by acts ratifying international agreements and conventions or else by Community regulations, with particular regard to

a) Act no. 388 of 30 September 1993, as subsequently amended, ratifying and implementing the accession protocols and agreements for the Schengen Agreement and the relevant Implementing Convention,

b) Act no. 93 of 23 March 1998, as subsequently amended, ratifying and implementing the Convention setting up the European Police Office (Europol),

c) EC Regulation no. 515/97 of the Council, of 13 March 1997, and Act no. 291 of 30 July 1998, as subsequently amended, ratifying and implementing the Convention on the Use of Information Technology for Customs Purposes,

[26] As amended by section 4(1) of legislative decree no. 109/2008 (implementing directive 2006/24/EC).

d) EC Regulation no. 2725/2000 of the Council, of 11 December 2000, setting up “Eurodac” to allow comparing fingerprints and ensure effective implementation of the Dublin Convention,

e) Chapter IV of Convention no. 108 on the protection of individuals with regard to the automated processing of personal data, as adopted in Strasbourg on 28 January 1981 and implemented by Act no. 98 of 21 February 1989, being the authority designated for the purpose of inter-State co-operation pursuant to Article 13 of said Convention.

3. The Garante shall co-operate with other independent administrative authorities in the performance of the relevant duties; to that end, the Garante may also invite representatives from another authority to take part in its meetings, or else be invited to take part in the meetings of another authority, and contribute to the analysis of issues of common interest. The Garante may also request the co-operation of specialized staff from another authority.

4. The Prime Minister and each Minister shall consult the Garante when drawing up regulations and administrative measures that are liable to produce effects on the matters regulated by this Code.

5. Subject to such shorter terms as may be provided for by law, the Garante’s opinion shall be rendered in the cases at stake within forty-five days of receiving the relevant request. Upon expiry of said term, the requesting administrative agency may proceed irrespective of the acquisition of the Garante’s opinion. If the term set out in this paragraph may not be complied with because of constraints related to preparation of the case, running of time may be suspended once only and the opinion shall have to be rendered in its final form within twenty days of receiving the information requested to the administrative agencies concerned.

6. A copy of any measure taken by judicial authorities in connection with either this Act or computer crime matters shall be transmitted to the Garante by the court clerk’s office.

CHAPTER II - THE GARANTE'S OFFICE

Section 155

(Applicable Principles)

1. In order to ensure accountability and autonomy pursuant to Act no. 241 of 07.08.90, as subsequently amended, and legislative decree no. 29 of 03.02.93, as subsequently amended, the Office of the Garante shall implement the principles concerning appointment and tasks of officials in charge of the individual cases, separation between guidance and supervisory tasks as conferred on the highest authorities and managerial tasks as committed to executive staff. The provisions of legislative decree no. 165/2001 shall also apply insofar as they are expressly referred to in this Code.

Section 156

(Permanent and Other Staff)

1. The Office of the Garante shall be under the authority of a secretary general who may also be a member of the ordinary or administrative judicature.

2. The permanent staff shall include one hundred employees.

3. The Garante shall set out, by its own regulations to be published in the Official Journal,

a) organisation and operation of the Office also with a view to discharging the tasks referred to in Section 154;
b) career patterns and recruitment in pursuance of the procedure laid down in Section 35 of legislative decree no. 165/2001;
c) allocation of staff to the different sectors and positions;
d) staff regulations and salaries by having regard to Act no. 249 of 31.07.97 as subsequently amended and, in respect of executive staff, Section 19(6) and 23-bis of legislative decree no. 165 of 30 March 2001, also taking account of specific functional and organisational requirements. Pending the general harmonisation of the salary conditions applying to independent administrative authorities, the staff of the Garante shall be granted eighty per cent of the salary paid to the staff employed by the Authority for Communications Safeguards;
e) administration and accounting mechanisms, also by derogating from the provisions applying to State accounts, the arrangements for using residuals including the amounts already entered as special accounting items, and the cases in which office charges or other types of consideration that are due on account of services delivered under the law shall be levied and used in accordance with Section 6(2) of Act no. 249 of 31 July 1997.

4. Staff from the State's civil service, other public administrative bodies or public entities in general may be employed by the Office for specific reasons. Said staff shall number twenty persons in all and include no more than twenty percent of executive staff; they shall be either assigned to temporary staff in accordance with the respective regulations or put on leave of absence pursuant to Section 13 of Presidential Decree no. 382 of 11.07.80 as subsequently amended. The corresponding number of posts shall be left available in the relevant permanent lists. The staff referred to herein shall be granted an allowance amounting to the difference, if any, between the salary paid by the administrative body or entity of origin and that granted to the permanent staff as based on a specific correspondence table that shall be adopted by the Garante. In no case shall said allowance be lower than fifty per cent of the salary already paid to the staff in question after deduction of special supplementary allowances.

5. In addition to the list of permanent staff, the Office may directly recruit no more than twenty employees on the basis of time-limited contracts, including the consultants hired on a temporary basis as per paragraph 7.

6. Section 30 of legislative decree no. 165/2001 shall apply.

7. Where necessary because of the technical or sensitive nature of the matters, the Garante may be assisted by consultants, who shall be paid in accordance with current professional fees or else employed via time-limited contracts for a period not in excess of two years, such contracts being renewable twice.

8. Staff and consultants working for the Office of the Garante shall be subject to secrecy rules as regards the information they may come to know in discharging their duties, where such information is to remain confidential.

9. The staff from the Office of the Garante in charge of the inquiries referred to in Section 158, numbering no more than five persons, shall be regarded as judicial police staff within the framework of the tasks committed and in accordance with the authority respectively vested in them.

10. The operating costs concerning the Garante shall be covered by a reserve set up for this purpose in the State budget and included as a specific item in the budget of the Ministry of Economy and Finance. The accounting reports shall be audited by the State Auditors' Department (*Corte dei Conti*).

CHAPTER III - INQUIRIES AND CONTROLS

Section 157

(Request for Information and Production of Documents)

1. In discharging its tasks, the Garante may request the data controller, the data processor, the data subject or a third party to provide information and produce documents.

Section 158

(Inquiries)

1. The Garante may order that data banks and filing systems be accessed and audits on the spot be performed as regards premises where the processing takes place or investigations are anyhow to be carried out with a view to checking compliance with personal data protection regulations.

2. The inquiries referred to in paragraph 1 shall be carried out by staff from the Office. The Garante may also avail itself, if necessary, of the co-operation of other State agencies.

3. The inquiries referred to in paragraph 1, if carried out at a person's home or in another private dwelling place and/or the relevant appurtenances, shall be carried out with the data controller's or data processor's informed consent. Alternatively, an authorisation from the judge presiding over the geographically competent court - by having regard to the place where the inquiries are to be carried out - shall be required, whereby the judge shall issue a reasoned decree without delay and anyhow by no later than three days after receiving the relevant request from the Garante if it can be proven that the inquiries cannot be postponed.

Section 159

(Arrangements)

1. The staff in charge of the inquiries shall be provided with an ID document and may be assisted, if necessary, by consultants bound by secrecy rules pursuant to Section 156(8). In carrying out measurements and technical operations, said staff may also make copies of papers, data and documents, also by samples and on computer media or else via electronic networks. Summary minutes of the inquiries shall be drawn up, also taking note of any declarations made by the persons attending them.

2. The entities concerned by the inquiries shall be given a copy of the authorisation issued by the judge presiding over the competent court, if any. They shall be required to allow the inquiries to be carried out and cooperate as necessary to that end. In case of denial, the inquiries shall be performed in any case and the expenses incurred shall be charged to the data controller by means of the provision finalising the relevant proceeding – which shall be regarded, as for this portion, to be an enforcement order pursuant to Sections 474 and 475 of the Civil Procedure Code.

3. If the inquiries are carried out at the data controller's or processor's premises, they shall be performed by informing either the data processor or, if the latter is absent or has not been designated, the persons in charge of the processing. Any person that has been designated by the data controller or processor to this effect may attend the inquiries.

4. No inquiries may be started either before 7 or after 20, except where provided otherwise in the authorisation issued by the judge presiding over the competent court; inquiries may also be carried out upon prior notice if this can facilitate their performance.

5. The information notices, requests and orders referred to in this Section and in Sections 157 and 158 may also be transmitted by e-mail or facsimile.

6. If the findings are such as to point to commission of an offence, Section 220 of the implementing, coordination and transitional provisions of the Criminal Procedure Code, as adopted by legislative decree no. 271 of 28.07.1989, shall apply.

Section 160

(Specific Inquiries)

1. As regards the data processing operations referred to in Titles I, II and III of Part II, the relevant inquiries shall be carried out by the agency of a member designated by the Garante.

2. Should the processing fail to comply with laws or regulations, the Garante shall draw the data controller's or processor's attention to the changes and additions that are required and verify that they are implemented. Where the request for the inquiries was made by the data subject, the latter shall be informed of the relevant outcome unless this may be prejudicial to actions or operations aimed at protecting public order and security or preventing and suppressing offences, or if there exist grounds related to State defence or security.

3. The inquiries may not be committed to others. Where necessary on account of the specific nature of the audit, the member designated as above may be assisted by specialized staff that shall be bound by secrecy rules as per Section 156(8). All records and documents, once acquired, shall be kept in such a way as to ensure their confidentiality and may be disclosed to the President and members of the Garante as well as to a limited number of employees in the Office, to be designated by the Garante pursuant to criteria laid down in the regulations as per Section 156(3), letter a), if this is necessary for the discharge of official duties.

4. As for inquiries concerning intelligence and security bodies or data that are covered by State secrecy, the designated member shall inspect the relevant records and documents and report on them orally during the meetings of the Garante.

5. In carrying out inquiries as per this Section with regard to judicial offices, the Garante shall take suitable arrangements in line with the respective powers and the specific institutional role of the authority in charge of the relevant proceeding. Inquiries concerning investigational records that are subjected to secrecy shall be postponed until secrecy is lifted, if so requested by the authority in charge of the proceeding.

6. Validity, enforceability and applicability of records, documents and measures related to judicial proceedings that are based on personal data processed by failing to comply with laws or regulations shall further be regulated by the relevant procedural provisions concerning civil and criminal matters.

TITLE III - SANCTIONS

CHAPTER I - BREACH OF ADMINISTRATIVE RULES

Section 161[27]

(Providing No or Inadequate Information to Data Subjects)

1. Breach of the provisions referred to in Section 13 shall be punished by a fine consisting in payment of between six thousand and thirty-six thousand Euro. The amount may be increased by up to three times as much if it is found to be ineffective on account of the offender's economic status.

[27] As amended by section 44(2) of decree no. 207/2008 dated 30 December 2008, converted with amendments into Act no. 14 dated 27 February 2009.

Section 162

(Other Types of Non-Compliance)

1. [28] Assigning data in breach of Section 16, paragraph 1, letter b), and/or other provisions concerning the processing of personal data shall be punished by a fine consisting in payment of between ten thousand and sixty thousand Euro.

2. [29] Breach of the provision referred to in Section 84(1) shall be punished by a fine consisting in payment of between one thousand and six thousand Euro.

2-bis. [30] If personal data are processed in breach of the measures set forth in section 33 and/or the provisions laid down in section 167, an administrative sanction shall be applied in all cases as consisting in payment of a fine ranging from ten thousand[31] to one hundred and twenty thousand Euro. Reduction of the applicable fine shall be ruled out in the cases referred to in section 33.

2-ter. In case of failure to abide by the provisions either setting out necessary measures or laying down prohibitions as per section 154(1), letters c. and d., respectively, an administrative sanction shall be applied in all cases as consisting in payment of a fine ranging from thirty thousand to one hundred and eighty thousand Euro.

2-quater. Any violation of the right to object in pursuance of the mechanisms set forth in Section 130(3-bis) and the respective regulations shall be punished in accordance with paragraph 2-bis hereof. [32]

Section 162-bis[33]

(Punishments Applying to Traffic Data Retention)

1. Any violation of the provisions set forth in section 132(1) and (1-bis) shall be punished by an administrative fine ranging from Euro 10,000 to 50,000, unless the facts at issue are established as a

[28] As amended by section 44(3)a. of decree no. 207/2008 dated 30 December 2008, converted with amendments into Act no. 14 dated 27 February 2009.
[29] As amended by section 44(3)b. of decree no. 207/2008 dated 30 December 2008, converted with amendments into Act no. 14 dated 27 February 2009
[30] This paragraph was added by section 44(3)c. of decree no. 207/2008 dated 31 December 2008, converted with amendments into Act no. 14 dated 27 February 2009
[31] As amended by Section 20-bis, paragraph 1, letter c., point 1, of Act no. 166 dated 20 November 2009, which also added paragraph 2-ter hereof.
[32] This paragraph was added by Section 20-bis, paragraph 1, letter c., point 2, of Act no. 166 dated 20 November 2009.
[33] This section was added by section 5(1) of Presidential decree no. 109/2008 (implementing directive 2006/24/EC). For the sake of completeness, the text of paragraph 2 of section 5 of the latter decree is reported hereinafter as referred to in Section 162-bis hereof: “Unless the fact is established as a criminal offence, failure to retain the data as per section 132(1) and (1-bis) of the Code, or retaining incomplete data, shall be punished by an administrative fine ranging from Euro 10,000 to 50,000, which may increased up to three times as much on account of the offender’s economic conditions. If the allocated IP address does not allow a subscriber or user to be identified uniquely, an administrative fine ranging from Euro 5,000 to 50,000 shall be imposed and may be increased up to three times as much on account of the offender’s economic conditions. The violations are established and the relevant sanctions imposed by the Ministry of Economic Development.”

criminal offence and without prejudice to section 5(2) of the legislative decree transposing directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006. [34]

Section 163 [35]

(Failure to Submit Notification or Submitting Incomplete Notification)

1. Whoever fails to timely submit the notification required under Sections 37 and 38 or provides incomplete information in a notification, in breach of his/her duties, shall be punished by a fine consisting in payment of between twenty thousand and one hundred and twenty thousand Euro.

Section 164 [36]

(Failure to Provide Information or Produce Documents to the Garante)

1. Whoever fails to provide the information or produce the documents requested by the Garante pursuant to Sections 150(2) and 157 shall be punished by a fine consisting in payment of between ten thousand and sixty thousand Euro.

Section 164-bis [37]

(Less Serious Cases and Aggravating Circumstances)

1. Where any of the violations referred to in sections 161 to 164 is less serious by having also regard to the social and/or business features of the activities at issue, the upper and lower thresholds set forth in the said sections shall be reduced to two-fifths thereof.

2. Where one or more provisions set forth in this Chapter – except for those referred to in Sections 162(2), 162-bis and 164 – are violated repeatedly, also on different occasions, in connection with especially important and/or large databases, an administrative sanction shall be applied as consisting in payment of a fine ranging from fifty thousand and three hundred thousand Euro. Reduction of the applicable fine shall not be allowed.

3. In other, more serious cases, in particular if the prejudicial effects produced on one or more data subjects are more substantial or if the violation concerns several data subjects, the upper and lower thresholds of the applicable fines as per this Chapter shall be doubled.

---

[34] As amended subsequently by Section 44(4) of decree no. 207/2008 dated 30 December 2008, converted with amendments into Act no. 14 dated 27 February 2009.
[35] As amended by Section 44(5) of decree no. 207/2008 dated 30 December 2008, converted with amendments into Act no. 14 dated 27 February 2009.
[36] As amended by Section 44(6) of decree no. 207/2008 dated 30 December 2008, converted with amendments into Act no. 14 dated 27 February 2009.
[37] This section was added by Section 44(7) of decree no. 207/2008 dated 30 December 2008, converted with amendments into Act no. 47 dated 27 February 2009.

4. The fines referred to in this Chapter may be increased by up to four times if they may prove ineffective on account of the offender's economic status.

Section 165 [38]

(Publication of Provisions by the Garante)

1. In the cases referred to in this Chapter, the additional administrative sanction may be applied as consisting in publication of the injunctive order, in whole or in part, in one or more newspapers as specified in the relevant provision. The offender shall be responsible for the said publication and bear the relevant costs.

Section 166

(Implementing Procedure)

1. The Garante shall be competent for receiving the report and imposing the sanctions referred to in this Chapter and in Section 179(3). Act no. 689 of 24 November 1981, as subsequently amended, shall apply as appropriate. Fifty percent of the annual proceeds shall be paid into the reserve fund referred to in Section 156(10) and shall only be used for discharging the tasks referred to in Sections 154(1), letter h), and 158.

CHAPTER II - CRIMINAL OFFENCES

Section 167

(Unlawful Data Processing)

1. Any person who, with a view to gain for himself or another or with intent to cause harm to another, processes personal data in breach of Sections 18, 19, 23, 123, 126 and 130 or else of the provision made further to Section 129 shall be punished, if harm is caused, by imprisonment for between six and eighteen months or, if the offence consists in data communication or dissemination, by imprisonment for between six and twenty-four months, unless the offence is more serious.

2. Any person who, with a view to gain for himself or another or with intent to cause harm to another, processes personal data in breach of Sections 17, 20, 21, 22(8) and (11), 25, 26, 27, and 45 shall be punished by imprisonment for between one and three years if harm is caused, unless the offence is more serious.

[38] As amended by Section 44(8) of decree no. 207/2008 dated 30 December 2008, converted with amendments into Act no. 14 dated 27 February 2009.

Section 168

(Untrue Declarations and Notifications Submitted to the Garante)

1. Whoever declares or attests to untrue information or circumstances, or else submits forged records or documents, in connection either with the notification referred to in Section 37 or with communications, records, documents or statements that are submitted or made, as the case may be, in a proceeding before the Garante and/or in the course of inquiries, shall be punished by imprisonment for between six months and three years, unless the offence is more serious.

Section 169

(Security Measures)

1. [39] Whoever fails to adopt the minimum measures referred to in Section 33 in breach of the relevant obligations shall be punished by detention for up to two years.

2. [40] A time limit shall be set either upon detecting the abovementioned offence or, in complex cases, by way of a subsequent provision issued by the Garante, for the offender to comply with the requirements referred to above. Said time limit shall not exceed the time span that is technically required; however, it may be extended in especially complex cases or else because of objective difficulties in complying, but it shall not be longer than six months. Within sixty days of the expiry of the above deadline, the offender shall be permitted by the Garante to pay one-fourth of the highest fine that can be imposed in connection with the administrative violation, on condition that the relevant requirements have been complied with. Compliance and performance of the abovementioned payment shall extinguish the offence. The body setting the time limit and the public prosecutor shall abide by the provisions made in Sections 21, 22, 23 and 24 of legislative decree no. 758 of 19.12.1994, as subsequently amended, insofar as they are applicable.

Section 170

(Failure to Comply with Provisions Issued by the Garante)

1. Whoever fails to comply with a provision issued by the Garante pursuant to Sections 26(2), 90, 150(1) and (2) and 143(1), letter c), in breach of the relevant obligations, shall be punished by imprisonment for between three months and two years.

---

[39] This paragraph was amended by Section 44(9), letter a., of decree no. 207/2008 dated 30 December 2008, converted with amendments into Act no. 14 dated 27 February 2009.
[40] This paragraph was amended by Section 44(9), letter b., of decree no. 207/2008 dated 30 December 2008, converted with amendments into Act no. 14 dated 27 February 2009

Section 171

(Other Offences)

1. Breach of the provisions referred to in Sections 113(1) and 114 shall be punished as provided for by Section 38 of Act no. 300 of 20 May 1970.

Section 172

(Additional Punishments)

1. Being convicted of any of the offences referred to in this Code shall entail publication of the relevant judgment.

TITLE IV - AMENDMENTS, REPEALS, TRANSITIONAL AND FINAL PROVISIONS

CHAPTER I - AMENDMENTS

Section 173

(Convention Implementing the Schengen Agreement)

1. Act no. 388 of 30 September 1993, as subsequently amended, ratifying and implementing the protocols and agreements for accession to the Schengen Agreement and the relevant Implementing Convention shall be amended as follows:

a) for paragraph 2 of Section 9 there shall be substituted the following:

"2. Any requests for access, rectification or erasure as well as for verification purposes referred to in Articles 109, 110 and 114(2) of the Convention, respectively, shall be made to the authority referred to in Section 1";

b) paragraph 2 of Section 10 shall be repealed;

c) for Section 11 there shall be substituted the following:

"11. 1. The supervisory authority referred to in Article 114 of the Convention shall be the Garante per la protezione dei dati personali. In discharging the tasks that have been committed to it under the law, the Garante shall carry out supervisory activities over data processing operations in pursuance of the Convention and shall carry out the controls referred to in said Article 114 also following a report and/or complaint lodged by a data subject that has received no adequate response to a request made in pursuance of Section 9(2), whenever no response can be provided to

said data subject on the basis of the information made available by the authority referred to in Section 9(1). 2. Section 10(5) of Act no. 121 of 1 April 1981, as subsequently amended, shall apply.";

d) Section 12 shall be repealed.

Section 174

(Service of Process and Judicial Sales)

1. In Section 137 of the Civil Procedure Code, after paragraph 2 there shall be inserted the following:

" If service on the recipient in person cannot be performed, the bailiff shall deliver or deposit a copy of the document to be served in a sealed envelope - except in the case referred to in Section 143(2) -, on which the relevant protocol number shall be written, and report this circumstance in the minutes appended both to the original document and to its copy. No marks or indications shall be placed on said envelope such as to allow inferring the contents of the relevant document.

The provisions referred to in paragraph 3 shall also apply to the communications performed via notes written by the court's clerk's office in pursuance of Sections 133 and 136."

2. In paragraph 1 of Section 138 of the Civil Procedure Code, for the words from "may always serve" up to "recipient" there shall be substituted the following : "*shall perform service, as a rule, by delivering a copy to the recipient in person, at the relevant dwelling place; alternatively, if this is not possible,".*

3. In paragraph 4 of Section 139 of the Civil Procedure Code, for the word "the original" there shall be substituted the following: "*a receipt".*

4. In Section 140 of the Civil Procedure Code, after the words "shall post a notice of deposit" there shall be inserted the following: *"in a closed, sealed envelope".*

5. Section 142 of the Civil Procedure Code shall be amended as follows:

a) paragraph 1 and 2 shall be replaced by the following: *"Subject to paragraph 2, if the recipient has no domicile, residence or place of abode in the State, has no domicile of choice or has appointed no attorney pursuant to Section 77, service shall be performed by mailing the document to the recipient with a registered letter and delivering a copy thereof to the public prosecutor, who shall be responsible for forwarding it to the Ministry for Foreign Affairs in order to have it delivered to the relevant addressee.";*

b) in the last paragraph, for the words "in the preceding paragraphs" there shall be substituted the following: *"in paragraph 1".*

6. In Section 143(1) of the Civil Procedure Code, the words from "and by means" up to the end of the sentence shall be deleted.

7. In Section 151(1) of the Civil Procedure Code, after the words "increased expeditiousness" there shall be added the following: *", confidentiality or protection of dignity"*.

8. In Section 250 of the Civil Procedure Code, after paragraph 1 there shall be added the following: *"The injunction referred to in paragraph 1 shall be delivered in a closed, sealed envelope if it is not delivered either to the recipient in person or by post"*.

9. In Section 490(3) of the Civil Procedure Code there shall be added the following sentence at the end: *"No reference to the debtor shall be made in the notice"*.

10. In Section 570(1) of the Civil Procedure Code, the words "of the debtor" shall be deleted and the words from "information" up to the end shall be replaced as follows: *"information also concerning the debtor's name may be provided by the court's clerk's office to any entity interested therein"*.

11. In Section 14(4) of Act no. 689 of 24 November 1981, as subsequently amended, there shall be added the following sentence at the end: *"If service cannot be performed on the recipient in person, the arrangements set out in Section 137(3) of said Code shall be abided by"*.

12. After Section 15 in Presidential Decree no. 445 of 28 December 2000, there shall be inserted the following:

"Section 15-bis. (Service of Records and Documents, Communications and Notices) 1. Section 137(3) of the Civil Procedure Code shall apply to service of records and documents by public administrative agencies on entities other than data subjects or persons designated by said data subjects as well as to service of communications and notices concerning the relevant contents. Summonses shall report such information as is strictly necessary for the relevant purpose.".

13. Section 148 of the Criminal Procedure Code shall be amended as follows:

a) paragraph 3 shall be replaced by the following:

"*3. Said document shall be served in full subject to different provisions under the law, a copy thereof being delivered, as a rule, either to the recipient or, if this is not possible, to the persons referred to in this Title. If service cannot be performed on the recipient in person, the bailiff or judicial police shall deliver a copy of the document to be served - unless service is to be performed on defence counsel or persons whose premises are the recipient's domicile of choice - after placing it inside an envelope that shall be sealed; the relevant protocol number shall be placed on the envelope and this circumstance shall be mentioned in the report appended both to the original and to the copy of the document in question."*;

b) after paragraph 5, the following shall be added:

"5-bis. Communications, notices and any other notes or summonses that are delivered in an open envelope to persons other than the recipients shall bear such indications as are strictly necessary.".

14. In Section 157(6) of the Criminal Procedure Code, for the words "is written on the outside of the envelope" there shall be substituted the following: *"shall be performed in the way described in Section 148(3)"*.

15. In Section 80 of the Implementing Provisions of the Criminal Procedure Code, as adopted by legislative decree no. 271 of 28 July 1989, for paragraph 1 there shall be substituted the following:

"1. If a copy of the search warrant is delivered to the caretaker and/or any person discharging the relevant tasks, Section 148(3) of the Code shall apply.".

16. Act no. 890 of 20 November 1982 shall be amended as follows:

a) in Section 2(1) there shall be added the following sentence at the end: *"No marks or indications shall be placed on the envelopes such as to allow inferring the contents of the relevant documents."*;

b) in Section 8(2), second sentence, after the words "The post officer shall leave a notice" there shall be added the following: *"in a closed envelope"*.

Section 175

(Police)

1. Processing operations that are performed with a view to transferring the data and information acquired in the course of administrative activities pursuant to Section 21(1) of Act no. 128 of 26 March 2001 as well as in view of the connections referred to in paragraph 3 of said Section shall be communicated to the Garante as per Section 39, paragraphs 2 and 3.

2. Personal data that were processed without electronic means by police bodies, public security agencies and other entities referred to in Section 53(1) prior to entry into force of this Code may be processed further upon implementation of this Code if it is established that they are accurate, complete and updated under the terms of Section 11.

3. For Section 10 of Act no. 121 of 1 April 1981 there shall be substituted the following:

"Section 10 (Controls)

1. Controls on the data processing centre shall be carried out by the Garante per la protezione dei dati personali pursuant to laws and regulations in force.
2. The data and information stored in the archives of the aforementioned centre may only be used in judicial or administrative proceedings upon acquisition of the original sources mentioned in Section 7(1), without prejudice to the provisions of Section 240 of the Criminal Procedure Code. If, during a judicial or administrative proceeding, the aforementioned data or information is found to be incorrect or incomplete or to have been processed unlawfully, the authority in charge of said proceeding shall inform the Garante per la protezione dei dati personali.
3. Any data subject may request the office referred to under subheading a) of Section 5(1) to confirm the existence of personal data relating to him/her, communicate such data in an intelligible form and, where said data are found to have been processed in breach of laws or regulations in force, have them erased or made anonymous.
4. Having carried out the necessary investigations, the office shall inform the applicant, by no later than twenty days after the date of the application, on the decision taken. The office may fail to respond if this may adversely affect actions or interventions for the protection of public security and

order or for preventing and suppressing criminal offences, and shall inform thereof the Garante per la protezione dei dati personali.

5. Where a person becomes acquainted with the existence of personal data relating to him/her that have been processed, with or without automated means, in breach of laws or provisions in force, said person may request the court of the data controller's place of residence to carry out the necessary inquiries and order rectification, completion, erasure or anonymisation of the data." .

Section 176

(Public Bodies)

1. In section 24(3) of Act no. 241 of 7 August 1990, after the words "by computerised means" there shall be inserted the following: *"except for the cases in which a data subject requests access to the personal data concerning him or her,"*.

2. In Section 2 of legislative decree no. 165 of 30 March 2001 concerning employment by public administrative agencies, after paragraph 1 there shall be inserted the following: *"1-bis. The organisational criteria referred to in this Section shall be implemented by complying with the provisions on processing of personal data."*.

3. For Section 4(1) of legislative decree no. 39 of 12 February 1993, as subsequently amended, there shall be substituted the following: *"1. The National Centre for Information Science in the Public Administration shall be hereby set up at the Prime Minister's Office with a view to implementing the policies made by the Minister for Innovation and Technology. Said Centre shall be autonomous as to its technical, operational, administrative, accounting and financial regulations and independent in its judgments."*.

4. Section 6 of legislative decree no. 39 of 12 February 1993 as well as the financing mechanisms in force within the framework of the budget drawn up by the Minister of Economy and Finance shall further apply to the National Centre for Information Science in the Public Administration.

5. For Section 5(1) of legislative decree no. 39 of 12 February 1993, as subsequently amended, there shall be substituted the following: *"1. Regulations applying to organisation, operation, personnel management, careers and expenditures shall be drawn up and submitted to the Prime Minister for adoption by the National Centre, subject to the constraints referred to in this decree."*.

6. As regards laws and regulations in force, for the words "Autorità per l'informatica nella pubblica amministrazione" there shall be substituted the words "Centro nazionale per l'informatica nella pubblica amministrazione [National Centre for Information Science in the Public Administration]".

Section 177

(Census Registers, Registers of Births, Deaths and Marriages, and Electoral Lists)

1. Local municipalities may only use the lists referred to in Section 34(1) of Presidential Decree no. 223 of 30 May 1989 for the public benefit also with regard to implementing the provisions on institutional communications.

2. For paragraph 7 in Section 28 of Act no. 184 of 4 May 1983, as subsequently amended, there shall be substituted the following: *"7. Access to said information shall not be allowed if a mother has objected to being referred to upon the child's birth in pursuance of Section 30(1) of Presidential Decree no. 396 of 3 November 2000."*.

3. Excerpts from the records included in the register of births, deaths and marriages as per Section 107 of Presidential Decree no. 396 of 3 November 2000 may only be provided to the entities that are the subject of such records, or else on the basis of a grounded request giving proof of the requesting party's personal, concrete interest with a view to defending a legal claim, or once seventy years have elapsed since the relevant record has been drawn up.

4. In Section 5(1) of Presidential Decree no. 223 of 20 March 1967, letters d) and e) shall be deleted.

5. In Section 51 of Presidential Decree no. 223 of 20 March 1967, for paragraph 5 there shall be substituted the following: *"A copy of the electoral list may be supplied for the purpose of implementing the provisions concerning electors and candidates, carrying out studies and statistical, scientific or historical researches, or researches in the social work sector, or else for purposes in the public interest."*.

Section 178

(Provisions Concerning the Health Care Sector)

1. In Section 27(3) and (4) of Act no. 833 of 23 December 1978, concerning the personal health card, after the words "the National Health Council" there shall be inserted the following words before the comma: *"and the Garante per la protezione dei dati personali"*.

2. Section 5 of Act no. 135 of 5 June 1990, concerning AIDS and HIV-related infections, shall be amended as follows:

a) for paragraph 1 there shall be substituted the following: *"1. Health care professionals and any other entities that are acquainted either with an AIDS case or with a case of HIV-related infection, also in the absence of the manifestations of disease, shall be required to provide the necessary assistance and take all the measures and precautions required to protect the data subject's rights and fundamental freedoms and dignity."*;

b) in paragraph 2, for the words "decree by the Minister of Health" there shall be substituted the following: *"decree by the Minister of Health, after consulting with the Garante per la protezione dei dati personali"*.

3. In Section 5(3) of legislative decree no. 539 of 30 December 1992, as subsequently amended, concerning medical drugs for human patients, there shall be inserted the following sentence at the end: *"At the expiry of said period, the pharmacist/chemist shall destroy the prescriptions in such a way as to prevent third parties from accessing the data they contain."*.

4. In Section 2(1) of the decree by the Minister of Health of 11 February 1997, as published in the Official Journal no. 72 of 27 March 1997, concerning imports of drugs registered abroad, letters f) and h) shall be deleted.

5. In Section 5-bis(1), first sentence, of decree-law no. 23 of 17 February 1998 as converted, with amendments, into Act no. 94 of 8 April 1998, for the words from "also concerns" to the end of the sentence there shall be substituted the following: *"shall be acquired jointly with the consent for the processing of personal data"*.

Section 179

(Other Amendments)

1. In Section 6 of Act no. 339 of 2 April 1958, the words *"keeping as confidential as necessary all the matters related to family life"* and *"ensuring respect for the employee's personality and moral freedom;"* shall be deleted.

2. In Section 38(1) of Act no. 300 of 20 May 1970, the words "4," and ", 8" shall be deleted.

3. In Section 12(3) of legislative decree no. 185 of 22 May 1999, concerning distance contracts, there shall be added the following words at the end: *"or, with regard to the infringement referred to in Section 10, to the Garante per la protezione dei dati personali"*.

[4.[41] Repealed.]

CHAPTER II - TRANSITIONAL PROVISIONS

Section 180

(Security Measures)

1.[42] The minimum security measures referred to in sections 33 to 35 and in Annex B) that were not laid down in Presidential Decree no. 318 of 28 July 1999 shall be taken by 31 March 2006.

2. Where a data controller is equipped with electronic means that, on the date of entry into force of this Code, do not allow the minimum measures as per Section 34 and the corresponding technical specifications referred to in Annex B to be immediately implemented in whole or in part, on

[41] This paragraph was repealed pursuant to Section 184 of legislative decree no. 42 dated 22 January 2004; the latter provision entered into force as of 1 May 2004 pursuant to section 183 thereof.
[42] This paragraph along with paragraph 3 hereof were amended by Section 3(1), letter a), of Decree-Law no. 158 of 24th June 2004, converted into Act no. 188 of 27th July 2004, by Section 6 of Decree-Law no. 266 of 9th November 2004, converted into Act no. 306 of 27th December 2004, by Section 6-bis of Act no. 26 of 1st March 2005 converting, with amendments, decree-law no. 314 of 30th December 2004, and by Section 1 of Act no. 51 of 23rd February 2006 converting, with amendments, decree-law no. 273 of 30th December 2005.

account of objective technical reasons, said data controller shall report the relevant reasons in a document bearing a certified date that shall be kept at his/her own premises.

3. In the case referred to in paragraph 2, the data controller shall take all possible security measures as related to the electronic means in his/her possession, so as to prevent an increase in the risks referred to in Section 31 also by means of suitable organisational, logistics or procedural measures. Said electronic means shall have to be brought into line with the provisions referred to herein by 30 June 2006.

Section 181

(Other Transitional Provisions)

1. As for processing operations concerning personal data that had started prior to 1 January 2004, by having regard to the initial implementing phase of this Code,

a)[43] the specification of the categories of data and operation pursuant to Sections 20(2) and (3) and 21(2) through ad-hoc regulations shall be provided, if not yet available, by 28 February 2007;

b) the decision to be made known to data subjects pursuant to Section 26(3), letter a), and 26(4), letter a), shall be adopted, if not yet available, by 30 June 2004;

c) the notification referred to in Section 37 shall be submitted by 30 April 2004;

d) the communications referred to in Section 39 shall be provided by 30 June 2004;

[e) Repealed.][44]

f) use of the forms referred to in Section 87(2) shall be compulsory as of 1 January 2005.

2. Section 21-bis of Presidential Decree no. 1409 of 30 September 1963, as added by Section 9 of legislative decree no. 281 of 30 July 1999, shall further apply until this Code comes into force.

3. The specification of data processing operations and data controllers as per Sections 46 and 53, to be included into Annex C), shall be provided by 30 June 2004 in the context of the initial implementation of this Code.

4. The information material supplied to the Garante in pursuance of Section 43(1) of Act no. 675 of 31 December 1996, which shall be used for the appropriate controls, shall continue being subsequently filed or destroyed based on the provisions in force.

5. The data subject's name and other identification data shall be omitted as per Section 52(4) from judgments and decisions rendered and/or made prior to entry into force of this Code at the data

[43] As amended by Section 3(1), letter c), of Decree-Law no. 158 of 24th June 2004, converted into Act no. 188 of 27th July 2004, and by Section 1 of Act no. 51 of 23rd February 2006 converting, with amendments, decree-law no. 273 of 30th December 2005, subsequently amended by Section 1 of the decree dated 12 May 2006 converted with amendments into Act no. 228 dated 12 July 2006, and finally by Section 6(1) of the decree dated 28 December 2006 converted with amendments into Act no. 17 dated 26 February 2007.

[44] This letter was repealed pursuant to Section 2-quinquies of Decree-Law no. 81 of 29th March 2004, converted into Act no. 138 of 26th May 2004.

subject's specific instance and with regard to documents that are published by means of electronic communications networks and/or the new products on paper or electronic media. The information systems that are used pursuant to Section 53(1) shall be brought into line with the aforementioned provision within 12 months of the coming into force of this Code.

6. Religious confessions that, prior to adoption of this Code, had laid down and adopted the safeguards referred to in Section 26(3), letter a), within the framework of their respective regulations, may continue processing data in compliance with said safeguards.

6-bis.[45] Pending enforcement of the measures and precautions required under Section 132(5), the term referred to in Section 4(2) of Legislative Decree no. 171 of 13th May 1998 shall apply to retention of telephone traffic data.

Section 182

(Office of the Garante)

1. With a view to ensuring continuity of institutional activities in the initial implementing phase of this Code, the Garante may, by no later than 31 March 2004,

a) set out the prerequisites for including into its permanent list of staff, at the initial level of the respective careers, staff permanently employed by public administrative agencies and/or public bodies that - on the date of publication of this Code - are employed by the Office of the Garante after being seconded from their respective administrations, by having regard to the available vacancies, and

b) provide that a certain number of posts, not exceeding thirty percent of the vacancies available in its permanent list of staff, are reserved in public competitions for non-permanent staff that have been employed by the Office of the Garante for at least one year.

CHAPTER III - REPEALS

Section 183

(Repealed Provisions)

1. As of the date of entry into force of this Code, there shall be repealed

a) Act no. 675 of 31 December 1996,

b) Act no. 325 of 3 November 2000,

c) legislative decree no. 123 of 9 May 1997,

d) legislative decree no. 255 of 28 July 1997,

[45] This paragraph was added by Decree-Law no. 354 of 24th December 2003, converted, with amendments, into Act no. 45 of 26th February 2004.

e) Section 1 of legislative decree no. 135 of 8 May 1998,

f) legislative decree no. 171 of 13 May 1998,

g) legislative decree no. 389 of 6 November 1998,

h) legislative decree no. 51 of 26 February 1999,

i) legislative decree no. 135 of 11 May 1999,

l) legislative decree no. 281 of 30 July 1999, except for Sections 8(1), 11 and 12,

m) legislative decree no. 282 of 30 July 1999,

n) legislative decree no. 467 of 28 December 2001,

o) Presidential Decree no. 318 of 28 July 1999.

2. As of the date of entry into force of this Code, there shall be repealed Sections 12, 13, 14, 15, 16, 17, 18, 19 and 20 of Presidential Decree no. 501 of 31 March 1998.

3. As of the date of entry into force of this Code, there shall also be or continue to be repealed

a) Section 5(9) of decree no. 279 by the Minister of Health of 18 May 2001, concerning rare diseases

b) Section 12 of Act no. 152 of 30 March 2001,

c) Section 4(3) of Act no. 52 of 6 March 2001, concerning bone marrow donors,

d) Section 16(2) and (3) of Presidential Decree no. 445 of 28 December 2000, concerning certifications of attendance at birth,

e) Section 2(5) of decree no. 380 by the Minister of Health of 27 October 2000, concerning information flows on discharged patients,

f) Section 2(5-quater 1), second and third sentence, of decree-law no. 70 of 28 March 2000 as converted, with amendments, into Act no. 137 of 26 May 2000, as subsequently amended, concerning the car accidents data bank for the insurance sector,

g) Section 6(4) of legislative decree no. 204 of 5 June 1998, concerning dissemination of data for purposes of research and co-operation in the scientific and technological sectors,

h) Section 330-bis of legislative decree no. 297 of 16 April 1994, concerning dissemination of data on pupils and students,

i) Section 8(4) and Section 9(4) of Act no. 121 of 1 April 1981.

4. As of the date on which the provisions laid down in the Code of conduct and professional practice referred to in Section 118 become effective, the retention time of personal data that is set

out in pursuance of Section 119, possibly by laws or regulations, shall be the one specified in said Code.

CHAPTER IV - FINAL PROVISIONS

Section 184

(Transposition of European Directives)

1. This Code shall implement Directive 95/46/EC of the European Parliament and of the Council, of 24 October 1995, and Directive 2002/58/EC of the European Parliament and of the Council, of 12 July 2002.

2. Whenever reference is made to Act no. 675 of 31 December 1996 by laws, regulations and other provisions, including those repealed by this Code, this shall be meant as a reference to the relevant provisions of this Code in accordance with the correspondence table annexed hereto.

3. Laws and regulations laying down more restrictive limitations or prohibitions on the processing of certain personal data shall be left unprejudiced.

Section 185

(Annexed Codes of Conducts and Professional Practice)

1. Annex A) shall contain, in addition to the Codes referred to in Section 12(1) and (4), the Codes whose adoption was encouraged by the Garante pursuant to Sections 25 and 31 of Act no. 675 of 31 December 1996, which had been published in the Official Journal of the Italian Republic prior to the date of issue of this Code.

Section 186

(Entry into Force)

1. This Code shall enter into force on 1 January 2004, except for Sections 156, 176, paragraphs 3, 4, 5, and 6, and 182, which shall enter into force on the day following publication of this Code. As of the latter date, the deadlines concerning complaints shall also apply as laid down in Sections 149(8) and 150(2).

This Code, bearing the State's Seal, shall be inserted into the Official Collection of Regulatory Provisions of the Italian Republic. It shall be for any person concerned to abide by it and ensure that it is abided by.

Done in Rome, this 27th day of June 2003.

ANNEXES

CODES OF CONDUCT (ANNEX A)

A.1 – PROCESSING OF PERSONAL DATA IN THE EXERCISE OF JOURNALISTIC ACTIVITIES

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Code of Practice Concerning the Processing of Personal Data in the Exercise of Journalistic Activities in Pursuance of Section 25 of Act no. 675 of 31.12.96

THE GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Having regard to Section 25 of Act no. 675 of 31.12.96, as amended by Section 12 of legislative decree no. 171 of 13.05.98, which provides that the processing of personal data in the exercise of the journalistic profession is to be carried out on the basis of a specific code of practice setting forth provisions and arrangements to safeguard data subjects by having regard to the nature of the data, especially as related to data disclosing health and sex life;

Having regard to para. 4-bis of said Section 25, which provides that the aforementioned code of practice shall also apply to the activity of freelance and trainee journalists and to any person who transiently processes personal data with a view to the occasional publication of papers, essays and other intellectual works;

Having regard to para. 2 of said Section 25, which provides that the code of practice is adopted by the National Council of the Press Association in cooperation with the Garante, which encourages such adoption and is responsible for having the code published in the *Official Journal* [Gazzetta Ufficiale];

Having regard to document no. 89/GAR of 26.05.97, in which the Garante called upon the National Council of the Press Association to adopt the code within six months of the date of transmission of said document;

Having regard to document no. 4640 of 24.11.97, in which the Garante granted the request for a short postponement of said six-month term as lodged by the National Council of the Press Association on 19.11.97;

Having regard to decision no. 5252 of 18.12.97, in which the Garante pointed to criteria that the National Council of the Press Association was called upon to consider in balancing freedoms and rights applying to journalistic activities;

Having regard to document no. 314 of 23.01.98, in which the Garante made additional considerations concerning the initial draft code as laid down by the National Council of the Press Association, which had been transmitted to the Garante by document no. 7182 of 30.12.97;

Having regard to document no. 204 of 15.01.98, in which - based on the initial implementation of Act no. 675/1996 and on the draft code - the Garante reported to the Minister of Justice on the desirability of amending Section 25 of the Act, which was actually amended by said legislative decree no. 171 of 13.05.98;

Having regard to document no. 5876 of 30.06.98, in which the Garante called upon the National Council of the Press Association to make further amendments to the draft approved of late by the Council at its meeting of 26th and 27th March 1998, as transmitted to the Garante by document no. 1074 of 08.04.98;

Having established adequacy of the provisions and arrangements laid down to safeguard data subjects in the final draft of the code of practice, as transmitted to the Garante by the National Council of the Press Association in document no. 2210 of 15.07.98;

Whereas the code of practice is to be published in the *Official Journal* under the Garante's responsibility, in pursuance of Section 25(2) of Act no. 675/1996, and enters into force fifteen days after its publication;

Hereby orders

The code of practice attached hereto to be transmitted to the Ufficio pubblicazione leggi e decreti [Publishing Department] of the Ministry of Justice in order for it to be published in the *Official Journal* of the Italian Republic.

Done in Rome this 29th day of July 1998

PRESS ASSOCIATION
National Council

CODE OF PRACTICE
Concerning the Processing of Personal Data in the Exercise of Journalistic Activities Pursuant to Section 25 of Act no. 675 of 31.12.96

(As published on the Official Journal No. 179 of 03.08.98)

Article 1
(General Principles)

1. These provisions are aimed at reconciling fundamental rights of individuals with citizens' right to information and freedom of the press.
2. The journalistic profession is carried out without being subject to authorisation or censorship as provided for by Article 21 of the Italian Constitution. On account of its being a prerequisite for freedom of the press, the fact of collecting, recording, keeping and disseminating information on facts and occurrences concerning persons, collective entities, official bodies, custom, scientific research and intellectual movements - when carried out within the scope of journalistic activity and for the relevant purposes - is essentially different in nature from the storage and processing of personal data by databases or other entities. The necessary derogations provided for by paragraphs

17 and 37 and Article 9 of Directive 95/46/EC of 24.10.95, of the European Parliament and the Council, and by Act no. 675/1996 are grounded on the aforementioned principles.

Article 2
(Data Banks Used by Editorial Offices and Protection of Journalists' Personal Archives)

1. Journalists collecting information for any of the operations referred to under Section 1(2)(b) of Act no. 675/96 must identify themselves, their profession and the purposes of the collection, unless this may endanger their safety or otherwise makes it impossible for them to carry out their journalistic activity; they must refrain from subterfuge and harassment. Having disclosed their activity, journalists are not required to provide the remaining items of information referred to in Section 10(1) of Act no. 675/96.
2. If personal data are collected from data banks used by editorial offices, publishing companies must inform the public at least twice a year, through advertisements, of the existence of such data banks and the place where the rights as per Act no. 675/96 may be exercised. Publishing companies must also include the data processor's name into management data in order for data subjects to apply to such processor for exercising the rights referred to in Act no. 675/96.
3. The safeguards set out in Section 2 of Act no. 69/1963 and Section 13(5) of Act no. 675/1996 with regard to sources of information apply to journalists' personal archives that are used for the exercise of professional activities and for the sole purposes related thereto.
4. Journalists may keep the data they have collected for as long as is necessary for the relevant professional purposes.

Article 3
(Protection of a Person's Residence)

1. Protection of a person's residence and other private places of abode also extends to health care, custodial or rehabilitation institutions in compliance with the relevant legislation and with the appropriate use of invasive techniques.

Article 4
(Rectification)

1. Journalists must promptly rectify mistakes or inaccuracies, also in pursuance of the duty of rectification in the cases provided for by law and in accordance with the relevant arrangements.

Article 5
(Right to Information and Personal Data)

1. In collecting personal data disclosing racial and ethnic origin, religious, philosophical or other beliefs, political opinions, membership of parties, trade unions, associations or organisations of a religious, philosophical, political or trade-unionist character and any data disclosing health and sex life, journalists must ensure the right to information on facts of public interest, by having regard to the materiality of such information, and avoid any reference to relatives or other persons who are not involved in the relevant events.

2. With regard to data concerning circumstances or events that have been made known either directly by the persons concerned or on account of their public conduct, the right to subsequently provide proof of the existence of lawful justification deserving legal protection is hereby left unprejudiced.

Article 6
(Materiality of the Information)

1. Disclosure of information of substantial public or social interest is not in conflict with the respect for private life if this information, detailed or not, is indispensable on account of either the originality of the relevant event(s) or the description of the specific way in which they have occurred as well as in the light of the qualifications of the persons involved.
2. The private sphere of prominent persons and persons holding public offices must be respected if the information or data are irrelevant to their role or public life.
3. Journalists' opinions and comments are part of freedom of the press as well as of the freedom of expression granted to all citizens by Constitution.

Article 7
(Protection of Children)

1. Journalists must not refer to the names of children involved in facts reported in the press or provide particulars allowing their identification, in order to protect their personality.
2. The protection of children's personality also extends to facts that are not specifically regarded as offences, by having regard to nature and items of the relevant report.
3. The child's right to privacy must always take precedence over both freedom of expression and freedom of the press; however, if journalists decide to publish reports or images concerning children for reasons of substantial public interest, without prejudice to legal constraints, they will be responsible for evaluating whether such publication does serve the child's objective interests in pursuance of the principles and limitations laid down in the "Treviso Charter".

Article 8
(Protection of Personal Dignity)

1. Without prejudice to materiality of the information, journalists must not provide information or publish images or photographs of persons involved in facts reported in the press where such information, images or photographs affect the persons' dignity, nor must they dwell on the details of acts of violence, unless the information or images are deemed to be important for the public.
2. Journalists must not film or produce images and photographs of persons in custody without the latters' consent, unless this is done either to serve a substantial public interest or for proven judicial and police purposes.
3. No person may be shown when fettered or handcuffed, unless this is necessary to report maltreatment.

Article 9
(Protection of the Right to Non-Discrimination)

1. In exercising the rights and duties related to freedom of the press, journalists must respect a person's right to non-discrimination on account of his/her race, religion, political opinions, sex, personal circumstances, bodily or mental condition.

Article 10
(Protection of the Dignity of the Ill)

1. In referring to the health of an identified or identifiable person, journalists must respect his/her dignity, right to privacy and decorum especially in cases involving severe or terminal diseases; they must avoid publishing analysis data of exclusively clinical interest.
2. Publication is allowed for the purpose of ensuring that all material information is disclosed and by respecting a person's dignity, if such person plays an especially important social or public role.

Article 11
(Protection of a Person's Sex Life)

1. Journalists must avoid reporting the sex life of any identified or identifiable person.
2. Publication is allowed for the purpose of ensuring that all material information is disclosed and by respecting a person's dignity, if such person plays an especially important social or public role.

Article 12
(Protection of Freedom of the Press with regard to Criminal Proceedings)

1. The limitation set out in Section 24 of Act no. 675/96 does not apply to the processing of data concerning criminal proceedings.
2. Processing of personal data disclosing adoption of the measures as per Section 686(1)(a) and (d), (2) and (3) of the Criminal Procedure Code is allowed within the scope of freedom of the press, in accordance with the principles laid down in Article 5.

Article 13
(Scope of Application and Disciplinary Measures)

1. These provisions shall apply to professional journalists, free-lance and trainee journalists and to any person carrying out journalistic activities even occasionally.
2. The disciplinary measures referred to under Title III of Act no. 69/1963 shall only apply to persons included in the Roll of Journalists, in the relevant lists or in the Register.

A.2 – PROCESSING OF PERSONAL DATA FOR HISTORICAL PURPOSES

CODE OF CONDUCT AND PROFESSIONAL PRACTICE

REGARDING THE PROCESSING OF PERSONAL DATA

FOR HISTORICAL PURPOSES

PREAMBLE

This Code is adopted by the public and private bodies mentioned below based on the following premises:

1) Any person accessing information and documents for historical purposes frequently uses personal data, which are protected by law in order to safeguard data subjects. In the light of the public interest related to the performance of said processing operations, whoever uses personal data for the aforementioned purposes (with particular regard both to public archives and to private archives declared to be of substantial historical interest in pursuance of Section 36 of Presidential decree no. 1409 of 30.09.63) was exempted by law from the obligation to request data subjects' consent pursuant to Sections 12, 20 and 28 of the Data Protection Act (*Act no. 675 of 31.12.96 – see, in particular, Section 27; legislative decree no. 135 of 11.05.99; legislative decree no. 281 of 30.08.99 – see, in particular, Section 7(4); presidential decree no. 1409 of 30.09.63 as subsequently amended and supplemented*).

2) Use of said data by users and archivists must therefore conform to both the relevant laws and this Code of conduct and professional practice; compliance with this Code is a fundamental prerequisite for the processing of data to be lawful, in addition to its being part of the relevant professional ethics (*Section 31(1), h), of Act no. 675 of 31.12.96; Section 6 of legislative decree no. 281 of 30.07.99*).

3) Compliance with the abovementioned rules should not affect investigations, research, gathering of documents and studies with regard to persons, facts and circumstances of the past, irrespective of the places in which said activities are performed.

4) Processing of personal data in connection with the conservation, categorisation and communication of documents kept both in State Archives and in historical Archives of public bodies is considered to be in the substantial public interest (*Section 23 of legislative decree no. 135 of 11.05.99*).

5) Adoption of this Code is encouraged by the Garante under the law pursuant to the principle of adequate representation of the public and private bodies concerned. This Code is also the expression of the professional associations and categories concerned, including scientific societies, with a view to reconciling the requirements of investigation into and description of historical facts with the rights and fundamental freedoms of data subjects (*Section 1, Act no. 675 of 31.12.96*).

6) In this Code provisions are made under the law concerning, in particular, *a)* rules based on fairness and non-discrimination in respect of users, to be abided by also in communication and dissemination of data, in line with the provisions applying to freedom of the press and freedom of speech; *b)* the specific safeguards applying to collection, consultation and dissemination of documents concerning data disclosing health, sex life or private family relations; *c)* modalities for applying the provisions on processing of data for historical purposes to private archives (*Section 7(5), legislative decree no. 281 of 30.07.99*).

7) Adoption of this Code is based not only on Articles 21 and 33 of the Constitution of the Italian Republic, but also on the relevant international sources and instruments concerning historical research and archives such as, in particular,:

a) Articles 8 and 10 of the 1950 *European Convention for the Protection of Human Rights and Fundamental Freedoms* as ratified by Italy with Act no. 848 of 04.08.55;

b) Council of Europe Recommendation No. R (2000) 13 of 13 July 2000;

c) Articles 1, 7, 8, 11 and 13 of the *Charter of Fundamental Rights of the European Union;*

d) the *Guidelines for a Law on Historical and Current Archives* as laid down by the International Council on Archives at the Ottawa Conference in 1996, and the *International Code of Ethics for Archivists* as adopted during the 1996 Beijing International Conference on Archives.

Chapter I
GENERAL PRINCIPLES

Article 1
(Purposes and Scope)

1. These provisions are aimed at ensuring that the use of personal data acquired in carrying out free historical research activities and in exercising the right to education and information, as well as in the course of the access to instruments and documents, takes place by respecting data subjects' rights, fundamental freedoms and dignity with particular regard to the right to privacy and personal identity.

2. This Code includes provisions applying to the processing of personal data for historical purposes in connection with documents that are kept either in archives of public administrative bodies, public bodies or in private archives which have been declared to be of substantial historical interest. This Code applies to all the processing operations concerning personal data that are performed by users for historical purposes, without the need for said users to subscribe to this Code.

3. This Code further includes guidelines for the conduct of any person processing, for historical purposes, personal data that are kept either in public archives or in private archives which have been declared to be of substantial historical interest; in particular,

a) as regards archivists, fairness and non-discrimination rules are laid down concerning users irrespective of their nationality, position, and education;

b) as regards users, safeguards are laid down concerning collection, use and disclosure of the data included in documents.

4. Owners, holders or keepers of either private archives which have not been declared to be of substantial historical interest or individual documents with historical interest may notify the competent Superintendent's Office for archives of their intention to apply this Code to the appropriate extent.

Article 2
(Definitions)

1. In implementing this Code, account shall be taken of the definitions and indications included in the legislation on personal data processing, with particular regard to the provisions mentioned in the Preamble. For the selfsame purposes,

a) "archivist" shall mean any natural or legal person, body or association that is responsible for supervising, acquiring, processing, preserving, restoring and managing historical, current and deposited archives of the public administration, private archives which have been declared to be of substantial historical interest as well as the private archives referred to in Article 1(4) above;

b) "user" shall mean any person either requesting access to or accessing documents including personal data for historical purposes, also in connection with journalistic activities and/or the occasional publication of papers, essays and other intellectual works;

c) "document" shall mean any item of information including personal data, whether in written or oral form or else stored on other media.

Chapter II
RULES APPLYING TO ARCHIVISTS' CONDUCT AND LAWFULNESS OF THE RELEVANT PROCESSING OPERATIONS

Article 3
(General Rules of Conduct)

1. Archivists processing personal data and the documents including such data shall take suitable measures, in line with the relevant laws and regulations, in order to ensure the respect for rights, fundamental freedoms and dignity of the persons to whom the processed data relate.

2. Archivists from public bodies or organisations shall ensure full compliance with the relevant laws and regulations concerning archives as also related to third parties with whom they have contacts because of their official duties or service – with particular regard to Sections 21 and 21-bis of presidential decree no. 1409 of 30.09.63 as amended by legislative decree no. 281 of 30.07.99 and Section 7 of said legislative decree no. 281/1999 and subsequently supplemented.

3. Any person discharging tasks related to archives in a public body shall process personal data by complying with such fairness, accuracy, impartiality honesty and diligence requirements as are warranted by professional practice and his/her position. He/She shall perform the relevant activities in accordance with the transparency criteria applying to public administrative agencies.

4. Any personal data that is used for historical purposes may be used further for said purposes. Such data shall be governed in principle by the same provisions irrespective of the documents including the data and the place of storage, without prejudice to the safeguards and precautions applying to specific categories of data or processing operation.

Article 4
(Conservation and Protection)

1. Archivists shall undertake:

a) to promote retrieval, acquisition and protection of documents. To that end, they shall follow such principles, methodologies and practice as are generally accepted and agreed upon in the relevant professional sector; they shall also see to systematically and continuously updating their historical, administrative and technological skills;

b) to safeguard integrity of archives and authenticity of documents, including those in electronic and multimedia form, and to aim at their permanent conservation with particular regard to the documents endangered by cancellation, dispersion and alteration of the data;

c) to ensure that reproductions be true to original documents and abstain from any activity aimed at tampering with, dissembling or misrepresenting facts, information, documents and data;

d) to ensure compliance with the security measures referred to in Section 15 of Act no. 675 of 31.12.96 and presidential decree no. 318 of 28.07.99, as subsequently amended and supplemented, by developing suitable measures in order to prevent destruction, dispersion or unauthorised access to documents and by also taking specific precautions in the light of certain risks – such as by only making available the copies of certain documents for consultation and keeping the relevant originals in a safe or an armoured cupboard.

Article 5
(Communication and Utilisation)

1. Archives shall be organised so as to ensure unrestricted utilisation of information sources.

2. Archivists shall ensure the widest possible access to archives and facilitate research and information gathering as well as retrieval of information sources in accordance with the applicable legislation.

3. Archivists shall inform researchers of any documents that have been removed from a file for the time being because of their being withheld from consultation.

4. Where data are collected by an archive on a systematic basis in cooperation with other public or private bodies in order to set up data banks including whole archive series, the relevant organisation shall make an ad-hoc agreement stipulating the arrangements for utilisation and the safeguards applying to data subjects in accordance with the law - in particular as regards the relationship

between data controller, processor and persons in charge of the processing as well as the relationships with third parties which may be interested in accessing the data.

Article 6
(Commitment to Confidentiality)

1. Archivists shall undertake:

a) to abstain from using, whether for their own research purposes or with a view to gain, information that is either unavailable to users or non-publicly available and has been obtained in the course of their activity even on a confidential basis. Archivists performing research activities for purposes of their own or else falling outside the scope of their professional activity shall be subjected to the same rules and limitations as apply to users;

b) to keep confidential any news and information concerning personal data they may come to know in the course of their activity.

2. Archivists shall further comply with the above confidentiality requirements after leaving their positions.

Article 7
(Data Update)

1. Archivists shall facilitate the exercise of a data subject's right to have the data updated, rectified or supplemented and ensure that the data are kept in a way allowing the original source to remain separate from any subsequent accessions.

2. With a view to the implementation of Section 13 in Act no. 675/1996, archivists shall make available the relevant search tools and sources in case a general request is made for access to a large series of data and/or documents; they shall further provide the person requesting it with appropriate directions to facilitate consultation.

3. In case a right is to be exercised pursuant to Section 13(3) of Act no. 675/1996 by an entity having an interest therein as regards personal data concerning either deceased persons or documents dating back to remote times, existence of the relevant interest shall be assessed by also taking account of the time already elapsed.

Article 8
(Oral Sources)

1. With regard to the processing of oral sources [of information], it shall be necessary for the interviewees to give their express consent, whether orally or not, even based on summary information including at least the interviewer's identity and activity and the purpose(s) of the data collection.

2. If an Archive acquires oral sources, it shall request the interviewer to produce a written statement to the effect that the purposes of the interview have been notified and the relevant consent has been obtained from the interviewees.

Chapter III
RULES OF CONDUCT FOR USERS AND LAWFULNESS OF THE RELEVANT PROCESSING OPERATIONS

Article 9
(General Rules of Conduct)

1. In accessing sources and exercising freedom of expression as well as in performing studies or research activities, users shall take such measures as are appropriate pursuant to laws and regulations in order to ensure respect for data subjects' rights, fundamental freedoms and dignity whenever they process personal data.

2. Pursuant to the provisions laid down in paragraph 1 above, users shall use documents under their own responsibility in compliance both with the purposes sought - which must be specified in the relevant research project - and with the principles laid down in Section 7 of legislative decree no. 281 of 30.07.99, stipulating that the data must be relevant and necessary.

Article 10
(Access to Public Archives)

1. Access to public archives shall be free. All users shall be entitled to accessing archives with the same rights and duties.

2. Pursuant to the laws in force, an exception shall be made for confidential documents concerning the State's home and foreign policy, which shall be made available after fifty years from the relevant date, as well as for documents including the data referred to in Sections 22 and 24 of Act no. 675/1996, which shall be made available after forty years from the relevant date. The term shall be seventy years in case of data disclosing health or sex life or private family relationships.

3. Consultation of the documents referred to in paragraph 2 may be authorised before expiry of the relevant term by the Ministry for Home Affairs, based on the opinion of either the competent State Archive Director or the competent Archives Superintendent and after hearing the Committee for Availability of Confidential Archive Documents at the Ministry for Home Affairs as provided for in Sections 8 and 9 of legislative decree no. 281/1999.

4. Where a permission for consultation of the documents referred to in paragraph 2 is requested by an user before expiry of the relevant term, a research project shall be submitted by that user to the body having the documents in its custody, in which the purposes of the research and the mechanisms for disclosure of the data shall be specified. The person making the request may provide such additional information as is deemed necessary.

5. The authorisation referred to in paragraph 3 shall be granted to all users who request it and fulfil the same conditions. The latter assessment shall be made on the basis of the research project referred to in paragraph 4.

6. In granting the authorisation referred to in paragraph 3 specific safeguards may be laid down in order to allow disclosure of the data without affecting data subjects' rights, freedoms and dignity.

7. In the light of the purposes of the research as specified in the relevant project, the above safeguards may also consist in the obligation not to disclose the persons' names, in only using the initials of data subjects' names, blanking the names in a data bank, temporarily withholding individual documents in a file or banning reproduction of documents. Special consideration shall be given to relevance of the data and to any reference to facts or circumstances allowing data subjects to be easily identified.

8. The authorisation referred to in paragraph 3 shall be granted to a specific person and the relevant holder may not delegate others to subsequently process the data. Documents shall retain their confidential nature and may not be used further by other entities without the relevant authorisation.

Article 11
(Disclosure)

1. The user's construction shall fall under the scope of the freedom of speech and expression as set out in the Constitution, without prejudice to the data subjects' right to privacy, personal identity and dignity.

2. In referring to a person's health, users shall refrain from publicising analytical data of exclusively clinical interest and describing the sex conduct relating to an identified or identifiable person.

3. The private sphere of either public figures or persons who have discharged public functions shall have to be respected if the news or data are irrelevant with regard to their role or public life.

4. Pursuant to Section 7(2) of legislative decree no. 281/1999, users shall take account of the relevance of the data at the time of their disclosure with particular regard to the individual personal data included in documents rather than to the documents as a whole. Users may disclose personal data if the latter are relevant and necessary for the research and do not affect the individuals' dignity and privacy.

5. Users are not required to provide the information as per Section 10(3) of Act no. 675/1996 where this would involve a clearly disproportionate effort.

6. Users may only use the processed data or the copies of documents including personal data that are accessible by a specific authorisation for the purposes of their own research; they shall be responsible for keeping the information confidential as also related to third parties.

Article 12
(Implementation)

1. By subscribing to this Code, public and private bodies including scientific societies and professional associations shall undertake to promote its widest possible dissemination and publicity and to ensure compliance, in accordance with the mechanisms and procedures laid down in the relevant regulations.

2. With regard to archives held by public bodies and private archives that have been declared to be of substantial historical interest, dissemination and implementation of this Code shall be ensured by the Superintendent's Offices for Archives.

Article 13
(Breach of the Rules of Conduct)

1. The competent administrative agencies shall apply the penalties laid down in the relevant regulations as regards public archives.

2. Societies and associations subscribing to this Code shall take suitable measures in case of a breach of its rules, based on the relevant by-laws and regulations, without prejudice to such punishments as are provided for by law.

3. Any breach by an user of the provisions laid down herein shall be notified to the entities which are entitled to granting the authorisation for consultation of confidential documents before the expiry of the lawful terms and shall be taken into account with a view to the granting of said authorisation. The competent administrative agency may also temporarily ban a person who has infringed the rules set out herein from accessing consultation rooms, in accordance with the relevant regulations. Such a person may also be refused any subsequent authorisation for the consultation of confidential documents.

4. As well as reporting any offence in accordance with the laws applying to civil servants, the entities referred to in paragraphs (1) and (2) may also inform the Garante concerning breaches of the rules laid down herein for the Garante to take such measures and impose such penalties as may be required.

Article 14
(Entry into Force)

1. This Code shall apply as of the fifteenth day following its publication on the *Official Journal* of the Italian Republic.

A.3 – PROCESSING OF PERSONAL DATA FOR STATISTICAL PURPOSES WITHIN THE FRAMEWORK OF THE SI.STA.N. [NATIONAL STATISTICAL SYSTEM]

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

PROVISION of 31 July 2002

Code of Conduct and Professional Practice Applying to the Processing of Personal Data for Statistical and Scientific Research Purposes within the Framework of the National Statistical System *(published in the Official Journal no. 230 of 01.10.2002)*

THE GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Having convened today, with the participation of Prof. Stefano Rodotà, President, Prof. Giuseppe Santaniello, Vice-President, Prof. Gaetano Rasi and Mr. Mauro Paissan, Members, and Mr. Giovanni Buttarelli, Secretary-General,

Having regard to Article 27 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, under which Member States and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper implementation of the national provisions adopted by the Member States pursuant to the Directive, taking account of the specific features of the various sectors,

Having regard to Section 31(1), letter h), of Act no. 675 of 31.12.1996, which entrusts the Garante with the task of encouraging, within the framework of the categories concerned and in compliance with the representation principle, the adoption of codes of conduct and professional practice for certain sectors, verifying that they are compliant with laws and regulations also by having regard to the considerations made by entities concerned, and contributing to ensuring that they are disseminated and respected,

Having regard to legislative decree no. 281 of 30.07.1999 on the processing of personal data for historical, statistical and scientific research purposes and, in particular, to Section 6(1) thereof, under which the Garante is entrusted with the task of encouraging adoption of one or more codes of conduct and professional practice for public and private entities, including scientific societies and trade associations, involved in the processing of data for statistical and scientific research purposes,

Having regard to Section 10(6) of the abovementioned legislative decree no. 281/1999, dealing with some aspects that should be specified in the code applying to the processing of data for statistical and scientific research purposes,

Having also regard to Section 12(2) of legislative decree no. 322 of 06.09.1989, as amended by Section 12(6) of legislative decree no. 281/1999, providing that the Committee for Safeguarding Statistical Information is to be heard with a view to the adoption of codes of conduct and professional practice in respect of the processing of personal data within the framework of the National Statistical System,

Having regard to the provision issued by the Garante on 10 February 2000, as published in the Official Journal no. 46 of 25.02.2000, in which the Garante encouraged adoption of one or more codes of conduct and professional practice in respect of the processing of personal data for statistical and scientific research purposes and called upon all the entities entitled to participate in the adoption of such codes under the representation principle to notify the Garante thereof by 31 March 2000,

Having regard to the communications received by the Garante in response to the provision of 10 February 2000, in which several public and private entities, scientific societies and trade associations indicated their intention to participate in drawing up the abovementioned codes, such entities having subsequently set up an ad-hoc working group including, inter alia, representatives from the following public bodies: Istituto Nazionale di Statistica – ISTAT [National Statistics Agency], Istituto di studi e analisi economica – ISAE [Institute for Economic Research and Analysis], Istituto per lo sviluppo della formazione professionale dei lavoratori – ISFOL [Institute for Development of Employees' Vocational Training], Presidenza del Consiglio dei Ministri – Dipartimento della Funzione Pubblica [Prime Minister's Office – Public Administration Department],

Whereas the draft code has been the subject of a wide-ranging discussion among the entities concerned, which have been given the opportunity to submit their considerations and put forward proposals,

Having regard to the Prime Minister's decree no. 152 of 09.03.2000, including provisions to set forth the criteria and procedure for determining the private bodies participating in the National Statistical System (SISTAN) pursuant to Section 2(1) of Act no. 125 of 28.04.1998,

Having regard to the Prime Minister's decree of 09.05.2001 on circulation of information within the National Statistical System,

Having regard to the Prime Minister's decree of 28.05.2002 on inclusion of additional statistics agencies into the SISTAN,

Having regard to the letter of 2 April 2001, by which the President of ISTAT forwarded, at the request of the Committee on Guidance and Coordination of Statistical Information, the text of the code of conduct and professional practice applying to the processing of personal data carried out for statistical and scientific research purposes within the framework of the National Statistical System, as undersigned by himself on behalf of the entities concerned,

Having regard to the decision made by this Authority concerning preliminary examination of the abovementioned code (decision no. 23 of 4 July 2001),

Considering that it is appropriate to proceed with the final assessment of the code of conduct and professional practice applying to the processing of personal data for statistical purposes within the framework of the SISTAN, also separately from the code that is to regulate use of personal data for statistical purposes outside the SISTAN in pursuance of Sections 6(1) and 10(6) of legislative decree no. 281/1999,

Having heard the Committee for Safeguarding Statistical Information as required by Section 12(2) of legislative decree no. 322 of 06.09.1989, also on the basis of the further analysis carried out in agreement with ISTAT,

Having taken account of the fact that compliance with the provisions laid down in the code is a fundamental prerequisite for the processing of personal data to be lawful,

Having ascertained that the code is compliant with laws and regulations concerning the protection of individuals with regard to the processing of personal data, in particular with Section 31(1), letter h), of Act no. 675/1996 as well as with Sections 6, 10, 11 and 12 of legislative decree no. 281/1999,

Whereas the code is to be published in the Official Journal of the Italian Republic under the Garante's responsibility, in pursuance of Section 6(1) of legislative decree no. 281/1999,

Having regard to the records on file,

Having regard to the considerations made by the Secretary General pursuant to Section 15 of the Garante's Regulations no. 1/2000 as adopted by decision no. 15 of 28 June 2000 and published in the Official Journal of the Italian Republic no. 162 of 13 July 2000,

Acting on the report submitted by Professor Gaetano Rasi,

HEREBY ORDERS

the annexed code of conduct and professional practice applying to the processing of personal data for statistical and scientific research purposes within the framework of the National Statistical System to be forwarded to the Law and Decree Publishing Department at the Ministry of Justice in order for it to be published in the Official Journal of the Italian Republic.

Done in Rome, the 31st of July 2002

The Chairman: Rodotà

ANNEX

CODE OF CONDUCT AND PROFESSIONAL PRACTICE APPLYING TO THE PROCESSING OF PERSONAL DATA FOR STATISTICAL AND SCIENTIFIC RESEARCH PURPOSES WITHIN THE FRAMEWORK OF THE NATIONAL STATISTICAL SYSTEM

Preamble

This Code is aimed at ensuring that use of personal data for statistical purposes, where such data are considered under the law to be in the substantial public interest and the source of official statistical information, and therefore are to be regarded as a community asset, is compliant with data subjects' rights, fundamental freedoms and dignity, and in particular with their right to confidentiality and personal identity.

This Code is adopted in pursuance of Sections 6 and 10(6) of legislative decree no. 281 of 30.07.1999 and applies to the processing operations for statistical purposes that are performed

within the framework of the National Statistical System with a view to the purposes referred to in legislative decree no. 322 of 06.09.1989.

Adoption of this Code is grounded on the relevant international sources and instruments concerning statistics, with particular regard to

a) The European Convention on the Protection of Human Rights and Fundamental Freedoms of 4 November 1950, as ratified by Italy via Act no. 848 of 04.08.1955,

b) The Charter of Fundamental Rights of the European Union of 18.12.2000, with particular regard to Articles 7 and 8 thereof,

c) Convention no. 108 as adopted in Strasbourg on 28.01.1981 and ratified by Italy via Act no. 98 of 21.02.1989,

d) Directive 95/46/EC of the European Parliament and of the Council of 24.10.1995,

e) Council of Europe Recommendation no. R(97)18 as adopted on 30.09.1997,

f) Article 10 of EC Regulations no. 322/97 as adopted by the Council of the European Union on 17.02.1997.

Organisations, agencies and entities applying this Code are required to also abide by the impartiality and non-discrimination principles in respect of other users, with particular regard to communication for statistical purposes of data that are stored in public archives and processed either by public bodies or with the help of public funds.

CHAPTER I

SCOPE AND GENERAL PRINCIPLES

Article 1
Scope

1. This Code shall apply to the processing of personal data for statistical purposes as carried out by

a) statistical organisations and agencies included and/or participating in the National Statistical System with a view to either implementing the national statistics programme or producing statistical information, in compliance with the respective institutional framework,

b) entities other than those mentioned under a), though belonging to the same administration/body, if the relevant processing operations are provided for by the national statistics programme and statistical agencies certify the methods adopted, by having regard to the provisions included in legislative decrees no. 322 of 06.09.1989 and no. 281 of 30.07.1999 - as subsequently amended and supplemented - in addition to those laid down herein.

Article 2
Definitions

1. For the purposes of this Code, the definitions set forth in Section 1 of Act no. 675 of 31.12.1996 – hereinafter referred to as the "Act" – and legislative decree no. 281 of 30.07.1999, including subsequent amendments and additions, shall apply. Additionally, for the same purposes

a) "processing for statistical purposes" shall mean any processing operation that is performed for the purpose of statistical analysis or the production, retention and dissemination of statistical results in pursuance of the national statistics programme, or else for the purpose of publicising statistical information within the scope of the institutional activities carried out by the entities referred to in Article 1,

b) "statistical result" shall mean the information obtained by means of the processing of personal data in order to quantify features of a collective phenomenon,

c) "public variable" shall mean the feature or set of features, whether qualitative or quantitative in nature, that is the subject of a statistical survey in which information included in public registers, lists, records, instruments and publicly available sources is used,

d) "statistical unit" shall mean the entity to which the processed data refer and/or can be referred.

Article 3
Data Subjects' Identifiability

1. For the purpose of implementing this code,

a) a data subject shall be considered to be identifiable if it is possible, by reasonable means, to establish a significantly likely relationship between the combination of the modalities for the variables concerning a given statistical unit and the latter's identification data,

b) the means that can be reasonably used to identify a data subject shall fall, in particular, under the following categories:

economic resources

time resources

files including personal data and other information sources including identification data jointly with a subset of the variables that are communicated and/or disseminated,

files, including or not personal data, providing information in addition to the data that are communicated and/or disseminated,

hardware and software to carry out the processing required in order to establish a connection between non-personal data and an identified entity, by having also regard to the actual possibility of unlawfully achieving identification of the latter entity in light of the security systems and monitoring software adopted,

knowledge of sample extraction, imputation, correction and statistical protection procedures as applied to obtain the data,

c) as regards communication or dissemination, a data subject shall be regarded as non-identifiable if the identification risk – in terms of likelihood of identifying the data subject by taking account of the communicated/disseminated data – is such that the means possibly required in order to achieve identification are to be considered disproportionate compared with the resulting infringement of and/or risk of infringing the data subject's rights, by having also regard to the benefit(s) that can be achieved.

Article 4
Criteria for Assessing the Identification Risk

1. With a view to the communication and dissemination of statistical results, the following criteria shall be considered in assessing the identification risk:

a) aggregate data shall be considered to consist in combinations of modalities associated either with a frequency that must not be lower than a pre-determined threshold, or with an intensity resulting from the synthesis of the values taken by a number of statistical units equal to said threshold. The minimum threshold value shall be three.

b) In assessing the threshold value account will have to be taken of the confidentiality level applying to the information.

c) Statistical results related exclusively to public variables are not subjected to the threshold rule.

d) The threshold rule may fail to be complied with if the statistical result does not reasonably allow identifying statistical units by having regard to assessment type and nature of the associated variables.

e) Statistical results concerning the same population may be disseminated in such a way as not to allow setting up connections among them and/or with other known information sources that may possibly permit identification.

f) Confidentiality is assumed to be adequately safeguarded if all the statistical units of a population show the same modality for a given variable.

2. The variables that may be disseminated in non-aggregate fashion shall be specified in the national statistics programme, where this is necessary to meet specific knowledge requirements also at international and/or Community level.

3. In communicating sample data collections, the identification risk shall be limited to the greatest possible extent. Said limit and the methodology to assess identification risk shall be set forth by ISTAT, which shall also lay down the arrangements for data release - in line with the principles referred to in Article 3(1), letter d) – and inform the Committee for Safeguarding Statistical Information.

Article 5
Processing of Sensitive Data by Private Entities

1. Private entities included in the National Statistical System pursuant to Act no. 125 of 28.04.1998 shall collect and further process sensitive data for statistical purposes in anonymous format, as a rule, subject to the provisions laid down in Section 6-bis(1) of legislative decree no. 322 of 06.09.1989 as inserted by legislative decree no. 281 of 30.07.1999 including subsequent amendments and additions.

2. Under certain circumstances, if lawful, specific statistical purposes related to the processing of sensitive data cannot be achieved without identifying data subjects, even on a temporary basis, the following prerequisites shall have to be met for said processing to be lawful:

a) the data subject must have given his/her own consent freely on the basis of the information provided;

b) the data controller must take specific measures in order to keep identification data separate already at the time of data collection, unless this proves unreasonable or requires a clearly disproportionate effort;

c) prior authorisation of the processing by the Garante is necessary, also on the basis of an authorisation applying to categories of data and/or types of processing; alternatively, the processing must be included in the national statistics programme.

3. Consent shall be given in writing. If the sensitive data are collected by specific methods such as telephone and/or computer-assisted interviews, which make it especially burdensome for the survey to obtain written consent, consent may be documented in writing on condition that is has been given expressly. In the latter case, the records giving proof of the information provided to the data subject as well as of the latter's consent shall be kept by the data controller for three years.

CHAPTER II

INFORMATION NOTICE, COMMUNICATION AND DISSEMINATION

Article 6
Information Notice

1. In addition to the information referred to in Section 10 of the Act, the data subject or the persons from which the data subject's personal data are collected for statistical purposes shall be notified of the possibility for the data to be processed for other statistical purposes in pursuance of legislative decrees no. 322 of 06.09.1989 and no. 281 of 30.07.1999 as subsequently amended and supplemented.

2. If the processing concerns personal data that have not been collected from the data subject and informing the latter entails a disproportionate effort compared with the right to be safeguarded – as per Section 10(4) of the Act –, the information shall be considered to have been notified if the processing is included in the national statistics programme or else is publicised by suitable means; the latter shall have to be communicated in advance to the Garante, which may provide for specific measures and arrangements.

3. As regards data collection for statistical purposes, informing the person the data are collected from on the specific purposes and the arrangements applying to the processing for which the data are intended may be postponed if this proves necessary in order to achieve the objectives of the relevant survey – by having regard to the subject matter and/or the nature of said survey -, on condition that the processing does not concern sensitive data. In such cases, the data subject must be provided with the supplementary information as soon as the reasons for which it has been withheld no longer apply – unless this entails a manifestly disproportionate effort. The entity responsible for the survey must draw up a document – to be subsequently kept for at least two years as of completion of the survey and made available to any entity exercising the rights referred to in Section 13 of the Act – detailing the specific reasons for which it has been considered appropriate to withhold the information, the

items of information that have been withheld and the arrangements followed to inform data subjects once the reasons for which said information has been withheld no longer apply.

4. Where the circumstances of the collection and the objectives of the relevant survey are such as to allow an entity to respond in the name and on behalf of another entity, being a relative of and/or cohabiting with the latter, the data subject may also be informed by the respondent.

Article 7
Communication to Entities Outside the National Statistical System

1. Individual data including no reference that can link them to data subjects may be communicated to entities outside the National Statistical System, in the form of sample collections and anyhow in such a way as to prevent data subjects from being identified.

2. Communication of personal data to university researchers and institutions, research bodies or members of scientific societies that fall under the scope of application of the code of conduct and professional practice on the processing of personal data carried out outside the National Statistical System for statistical and scientific research purposes – as per Section 10(6) of legislative decree no. 281 of 30.07.1999 including subsequent amendments and additions – shall be allowed within the framework of specific laboratories set up by entities included in the National Statistical System, on condition that

a) the data result from processing operations, for which the abovementioned entities included in the National Statistical System act as data controllers,

b) the data to be communicated do not include identification data,

c) the provisions on statistics secrecy and personal data protection as included, inter alia, in this code are complied with by the researchers accessing said laboratories, also on the basis of a prior commitment statement,

d) access to laboratories is controlled and monitored,

e) access to files including data other than those that are communicated is not permitted,

f) suitable measures are taken in order for the researchers using the laboratories to be prevented from performing data entry and retrieval,

g) releasing the results of the processing operations performed by researchers using the laboratories is only authorised after the relevant laboratory staff have verified compliance with the provisions as per point c).

3. Within the framework of joint projects that are also aimed at pursuing institutional purposes as related to the data controller of the processing that has given rise to the data, the entities included in the National Statistical System may communicate personal data to researchers working on behalf of universities, other public bodies and organisations pursuing research purposes, provided the conditions below are complied with:

a) the data result from processing operations, for which the abovementioned entities included the National Statistical System act as data controllers,

b) the data to be communicated do not include identification data,

c) the communication takes place in accordance with ad-hoc research protocols undersigned by all the researchers participating in the specific project,

d) the provisions concerning statistics secrecy and personal data protection as also included in this code are expressly laid down in the abovementioned protocols to the effect that they should be binding on all the researchers participating in the specific project.

4. Researchers authorised to communicate data are banned from carrying out processing operations for purposes other than those expressly referred to in the research protocol, keeping the communicated data beyond the project deadline and communicating the data further to third parties.

Article 8
Data Communication between Entities Included in the National Statistical System

1. Communication of personal data including no identification data is allowed within the framework of entities included in the National Statistical System as regards the statistical processing operations that are instrumental to achieving the requesting party's institutional purposes and have been expressly referred to in the relevant request, without prejudice to compliance with the requirement that data should be relevant and not excessive.

2. Communicating, inter alia, the identification data of statistical units is allowed within the framework of entities included in the National Statistical System if the requesting party declares that no identical statistical result can be obtained otherwise, subject to lodging of a reasoned request in which the purposes to be achieved pursuant to legislative decree no. 322 of 06.09.1989, including the scientific research purposes as regards the entities referred to in Section 2 of said decree, are detailed – without prejudice to compliance with the requirement that data should be relevant and absolutely necessary.

3. Such data as are communicated in pursuance of paragraphs 1 and 2 above may only be processed by the requesting party, even subsequently, for the purposes sought under legislative decree no. 322 of 06.09.1989, including the scientific research purposes as regards the entities referred to in Section 2 of said decree, in accordance with the limitations set forth in legislative decree no. 281 of 30.07.1999 and by complying with the security measures referred to in Section 15 of the Act as subsequently amended and supplemented.

Article 9
Supervisory Authority

1. The Committee for Safeguarding Statistical Information referred to in Section 10 of legislative decree no. 322 of 06.09.1989 shall contribute to appropriately implementing the provisions laid down in this code with particular regard to the provisions made in Article 8 above, by reporting possible breaches to the Garante.

CHAPTER III

SECURITY AND RULES OF CONDUCT

Article 10
Data Collection

1. The entities referred to in Article 1 shall take special care in selecting the staff in charge of collecting data as well as in laying down organisation and mechanisms for the survey, so as to ensure compliance with this code and protection of data subjects' interests; they shall also take steps to appoint the persons in charge of the processing as required by law.

2. At all events, the staff in charge of data collection shall abide by the provisions laid down herein as well as by the instructions received. In particular,

a) they shall disclose their identity, their tasks and the purposes of the collection also by means of suitable documents,

b) they shall provide the information as per Section 10 of the Act and Section 6 of this Code, and such additional explanations as may allow data subjects to answer in a suitable, informed manner, and shall refrain from following deceptive practices or putting undue pressure on data subjects,

c) they shall not carry out data surveys simultaneously on behalf of several data controllers, except where this is expressly authorised,

d) they shall timely correct mistakes and inaccuracies in the information acquired with the survey,

e) they shall take special care in collecting the personal data referred to in Sections 22, 24 and 24-bis of the Act.

Article 11
Data Retention

1. Personal data may be retained longer than is necessary to achieve the purposes for which they have been collected and/or subsequently processed in pursuance of Section 9 of the Act as well as of Section 6-bis of legislative decree no. 322 of 6 September 1989, as subsequently amended and supplemented. In those cases, identification data may be retained for as long as they are necessary with a view to:

continuous and longitudinal surveys,

control, quality and coverage surveys,

identification of sample patterns and selection of survey units,

setting up archives of statistical units and information systems,

other cases in which this is fundamental and can be adequately documented for the purposes sought.

2. In the cases referred to in paragraph 1, identification data shall be stored separately from all other data so as to allow different levels of access, unless this proves impossible on account of the specific

features of the processing or involves an effort that is clearly disproportionate compared with the right to be protected.

Article 12
Security Measures

1. In taking the security measures as per Section 15(1) of the Act and the Regulations referred to in paragraph 2 of the latter Section, the data controller shall also specify the different levels of access to the personal data by having regard to their nature and the tasks discharged by the entities involved in the processing.

2. The entities referred to in Section 1 shall take the precautions required under Sections 3 and 4 of legislative decree no. 135 of 11 May 1999 with regard to the data referred to in Sections 22 and 24 of the Act.

Article 13
Exercising Data Subject's Rights

1. As for exercising the rights referred to in Section 13 of the Act, any data subject may access the statistical archives containing the data concerning him/her to have them updated, rectified or supplemented, provided that this does not prove impossible on account of the nature or status of the processing or else involves an effort that is clearly disproportionate.

2. Pursuant to Section 6-bis of legislative decree no. 322 of 6 September 1989, the data processor shall take note of the changes requested by a data subject using ad-hoc fields and/or registers without modifying the data initially entered, where these operations do not produce significant effects either on statistical analysis or on the statistical results related to the processing. In particular, no changes shall be made if the latter are in conflict with statistical classifications and methodology as adopted in pursuance of international, Community and national regulations.

Article 14
Rules of Conduct

1. Data processors and persons in charge of the processing shall also follow the rules of conduct detailed below, where they may lawfully access – also for reasons related to their work, study and research – personal data that are processed for statistical purposes:

a) personal data may only be used for the purposes specified in planning the processing operations,

b) personal data shall be kept in such a way as to prevent their being dispersed, stolen or anyhow used by departing from either the relevant laws or the instructions received,

c) personal data and information that is not publicly available, where acquired in the course of performing statistical activities and/or activities instrumental to the latter, may not be disseminated or used otherwise for private purposes,

d) the activities performed shall be adequately documented,

e) professional know-how concerning personal data protection shall be continuously adjusted to technological and methodological evolution,

f) communication and dissemination of statistical results shall be encouraged as related to users' information requirements on condition that personal data protection regulations are complied with.

2. The data processors and persons in charge of the processing referred to in paragraph 1 shall have to abide by the provisions laid down herein, also if they are not bound by official and/or professional secrecy rules. Data controllers shall take suitable measures in order to ensure that data processors and persons in charge of the processing are familiar with the abovementioned provisions.

3. Any conduct that fails to comply with the rules set forth herein shall have to be immediately reported either to the data controller or to the data processor.

A.4 – PROCESSING OF PERSONAL DATA FOR STATISTICAL AND SCIENTIFIC PURPOSES

(Published in the Official Journal no. 190 of August 14, 2004)

The Garante per la protezione dei dati personali

Having convened today, with the participation of Prof. Stefano Rodotà, President, Prof. Giuseppe Santaniello, Vice-President, Prof. Gaetano Rasi and Mr. Mauro Paissan, members, and Mr. Giovanni Buttarelli, secretary-general,

Having regard to Article 27 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, under which Member States and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper implementation of the national provisions adopted by Member States pursuant to the Directive, taking account of the specific features of the various sectors;

Having regard to Section 12 of the personal data protection Code (legislative decree no. 196 of June 30, 2003), which entrusts the Garante with the task of encouraging, within the framework of the sectors concerned and in accordance with the principle of representation as well as with the guidelines set out in the Council of Europe's recommendations on processing of personal data, the adoption of codes of conduct and professional practice in respect of certain sectors, verifying that they are compliant with laws and regulations, also in the light of the remarks submitted by the entities concerned, and contributing to ensure that they are disseminated and abided by;

Having regard to Section 106(1) of the Code, which entrusts the Garante with the task of encouraging adoption of one or more codes of conduct and professional practice for public and private entities, including scientific societies and professional associations, involved in processing data for statistical or scientific purposes;

Having regard to Section 106(2) of the said Code, concerning some issues that have to be addressed by the code of conduct and professional practice applying to processing of data for statistical and scientific purposes, on the basis of some safeguards;

Having regard to the provision of February 10, 2000 by the Garante per la protezione dei dati personali, published in the Official Journal of the Italian Republic no. 46 of February 25, 2000, whereby the Garante encouraged adoption of one or more codes of conduct and professional practice concerning processing of personal data for statistical and scientific research purposes and called upon all the entities entitled to participate in the adoption of said codes under the representation principle to notify the Garante thereof;

Having regard to the communications received by the Garante further to the aforementioned provision of February 10, 2000, in which several public and private entities, scientific societies and professional associations notified that they intended to participate in adoption of the codes, whereupon an ad-hoc working group was set up including, in particular, representatives from the following entities: Conferenza dei rettori delle università italiane; Italian Epidemiologists' Association; Italian Sociologists' Association; Italian Council for Social Science; Italian Economists' Society; Italian Biometrics Society; Italian Historical Demography Society; Italian

Society for Hygiene, Preventive Medicine, and Public Health; Italian Statistics Society; Italian Society of Medical Statistics and Clinical Epidemiology; Association of the Institutions and Bodies Carrying out Market Surveys, Opinion Polls, and Social Researches;

Whereas the text of the code was disseminated broadly also via its publication on this Authority's website, as communicated by a notice in the Official Journal of the Italian Republic of May 20, 2004, in order to foster the widest possible discussion and allow gathering remarks and suggestions from all the entities concerned;

Having regard to the remarks and suggestions received further to the aforementioned notice;

Whereas compliance with the provisions laid down in the code of conduct and professional practice is a fundamental precondition for the processing of personal data by public and private bodies to be lawful and fair (Section 12(3) of the Code);

Having found that the code of conduct and professional practice is compliant with the laws and regulations on personal data protection, also by having regard to Sections 12, 104 and following ones of the Code,

Whereas under Section 12(2) of the Code, the code of conduct and professional practice is to be published in the Official Journal of the Italian Republic under the Garante's responsibility and included in Annex A to said Code pursuant to a decree by the Minister of Justice;

Having regard to the official records;

Having regard to the considerations made by the Secretary General pursuant to Section 15 of the Garante's Regulations no. 1/2000, as adopted by resolution no. 15 of June 28, 2000 and published in the Official Journal of the Italian Republic no. 162 of July 13, 2000;

Acting on the report submitted by Prof. Gaetano Rasi,

ORDERS

the annexed code of conduct and professional practice applying to processing of personal data for statistical and scientific purposes to be forwarded both to the Ufficio pubblicazioni leggi e decreti of the Ministry of Justice in order for it to be published in the Official Journal of the Italian Republic, and to the Minister of Justice in order for it to be included in Annex A) to the Code.

Done in Rome, this 16th day of June 2004

THE PRESIDENT
Rodotà

THE RAPPORTEUR
Rasi

THE SECRETARY GENERAL
Buttarelli

ANNEX

CODE OF CONDUCT AND PROFESSIONAL PRACTICE APPLYING TO PROCESSING OF PERSONAL DATA FOR STATISTICAL AND SCIENTIFIC PURPOSES

This Code was undersigned by:

- Conferenza dei rettori delle università italiane;
- Italian Epidemiologists' Association;
- Italian Sociologists' Association;
- Italian Council for Social Science;
- Italian Economists' Society;
- Italian Biometrics Society;
- Italian Historical Demography Society;
- Italian Society for Hygiene, Preventive Medicine, and Public Health;
- Italian Statistics Society;
- Italian Society of Medical Statistics and Clinical Epidemiology;
- Association of the Institutions and Bodies Carrying out Market Surveys, Opinion Polls, and Social Researches

PREAMBLE

We, the undersigned private and public entities, hereby adopt this Code pursuant to the provisions made in Section 106 of legislative decree no. 196 of June 30, 2003 containing the personal data protection Code (hereinafter referred to as the "decree"), on the basis of the following premises:

1) The provisions of this Code of conduct and professional practice are aimed at reconciling the individual's fundamental rights and freedoms, in particular the right to personal data protection and the right to privacy, with the requirements of statistics and scientific research as deriving from the principle of freedom of research set forth in the Constitution, which is a precondition for scientific development, improvement of individuals' life-styles, and the growth of a democratic society;

2) Researchers working, whether alone or jointly with others, within universities, research bodies and institutions, and scientific societies, shall abide by this Code in all stages of processing personal data for statistical and/or scientific purposes regardless of whether the respective bodies and scientific societies have undersigned this Code;

3) In implementing this Code, its addressees shall comply with the principles set out in the 1950 European Convention for the Protection of Human Rights and Fundamental Freedoms as ratified by Act no. 848 of August 4, 1955, in EC Directive 95/46 of the European Parliament and of the Council, in Council of Europe's Recommendations No. R(83)10 adopted on September 23, 1983 and No. R(97)18 adopted on September 30, 1997, and in other Community and international instruments concerning processing of personal data for statistical and scientific purposes. They shall abide by the principle whereby data should be relevant and not excessive, meaning that the planned processing should not be redundant compared with the purposes sought by having regard both to the available data and to the processing operations that have already been carried out by the relevant controller;

4) As for the matters that are not regulated by this Code, the provisions laid down in personal data protection legislation shall apply as also related to the data controller's public or private nature (see Sections 18 and following ones and 23 and following ones of the decree). In particular, no personal data that is processed for statistical or scientific purposes may be used to take decisions and/or measures in respect of the data subject, or else with a view to processing operations for purposes of a different kind;

5) Processing for statistical purposes shall mean any and all processing operations that are performed for purposes of statistical investigation and/or the production of statistical results, also by means of statistical information systems (Section 4 of the decree);

6) Processing for scientific purposes shall mean any and all processing operations that are performed for purposes of study and systematic research with a view to developing scientific knowledge in a specific sector (Section 4 of the decree);

7) Entities and bodies applying this Code shall abide by the impartiality and non-discrimination principle with regard to any other entities that process the data for statistical and/or scientific purposes. In undersigning this Code, special attention shall be paid, in particular, to the importance of said principle in connection with communications for statistical and/or scientific purposes of data that have been either deposited with public archives or processed on the basis of public funds;

8) The decree and this Code shall not apply to anonymous data;

9) The provisions laid down in the codes of conduct and professional practice referred to in Sections 118 and 140 of the decree shall apply to processing operations for purposes of commercial information and communication including the related market surveys.

Chapter I – SCOPE AND GENERAL PRINCIPLES

Article 1. Definitions

1. For the purposes of this code, the definitions set out in Section 4 of the decree shall apply with the following additions:

a) “statistical result” shall mean the information obtained by processing personal data in order to quantify components of a collective phenomenon;

b) “statistical unit” shall mean the entity the processed data relate and/or can be related to;

c) “indirectly identifying data” shall mean a set of modalities of characters that are or can be associated with a statistical unit in such a manner as to allow it to be identified with the use of reasonable time and resources pursuant to the principles referred to in Section 4;

d) “public variable” shall mean the character or the combination of characters of a qualitative and/or quantitative nature that is the subject of a statistical survey related to information contained in public registers, lists, instruments, documents, or publicly available sources;

e) “research body or institution” shall mean any private or public entity that pursues statistical and/or scientific research purposes within the framework of its institutional purposes, and whose scientific activity can be documented;

f) “scientific society” shall mean an association among scholars in a given sector, including the respective professional associations.

2. Except where specified otherwise, any reference to processing operations for statistical purposes shall also include processing operations for scientific purposes.

Article 2. Scope of Application

1. This Code shall apply to all the processing operations carried out for statistical and scientific purposes – pursuant to the relevant sector-related methodological standards – in respect of which universities, other research bodies or institutions, and scientific societies, as well as researchers working within the framework of said universities and research bodies and institutions, and members of said scientific societies, act as data controllers.

2. This Code shall not apply to processing operations for statistical and scientific purposes that are related to activities aimed at safeguarding health as carried out by health care professionals and/or health care bodies, including such activities as are comparable in terms of significant personalised impact on the data subject. Said processing operations shall continue to be regulated by the relevant provisions.

Article 3. Prerequisites for the Processing

1. Any research shall be carried out on the basis of a project to be drawn up according to the relevant sector-related methodological standards, also in order to prove that the processing is performed for suitable, actual statistical or scientific purposes.

2. The research project referred to in paragraph 1 shall additionally

a) specify the measures to be adopted in processing personal data with a view to ensuring respect for this code as well as for personal data protection legislation;

b) designate the data processors, if any;

c) contain a statement whereby the entities concerned undertake to abide by the provisions of this code. A similar statement shall be also rendered by the entities – researchers, data processors, and persons in charge of the processing – involved in the continuation of the relevant research, and shall be kept pursuant to the provisions made in paragraph 3.

3. The data controller shall deposit the project with the respective university, research body, or scientific society. The latter shall be in charge of keeping it for five years as of the planned completion of the research, by ensuring its confidentiality – access to the project being only permitted for the purpose of applying personal data protection legislation.

4. When processing data suitable for disclosing health, the entities concerned shall comply with the confidentiality and security rules health care professionals are required to apply, or else with comparable confidentiality and security rules.

Article 4. Identificability of Data Subjects

1. For the purpose of applying this Code,

a) a data subject shall be considered to be identifiable if a significantly likely association can be established – by using reasonable means – between the combination of the modalities of the variables relating to a statistical unit and the identification data of the latter unit;

b) the means that can be reasonably used to identify a data subject relate, in particular, to the following categories:

- economic resources;
- time resources;
- personal data filing systems and/or other information sources containing identification data jointly with a subset of the variables that are communicated and/or disseminated;
- filing systems also not including personal data where they provide additional information to the one that is communicated or disseminated;
- hardware and software resources to perform the processing required in order to relate non-personal information to an identified entity, also by taking account of the actual possibility to unlawfully achieve identification of said entity in light of the security systems and control software that have been implemented;
- knowledge of the procedures for sample extraction, statistical imputation, correction and protection as adopted with a view to data production;

c) in case of communication and/or dissemination, a data subject may be regarded as not identifiable if the identification risk – in terms of likelihood of identifying said data subject by having regard to the data that have been communicated and/or disseminated – is such that the means possibly required to effect identification are to be considered disproportionate compared with the (risk of) damage resulting therefrom to the data subjects' rights, also in the light of the benefit(s) that might be achieved.

Article 5. Criteria to Assess the Identification Risk

1. For the purpose of communicating and disseminating data, the following criteria shall be taken into account in assessing the identification risk:

a) aggregated data shall be combinations of modalities either with a frequency that is not lower than a given threshold or with an intensity resulting from the sum of the values taken by as many statistical units as the said threshold. The minimum value that may be set for the threshold in question shall be three;

b) in assessing the threshold level account shall be taken of the confidentiality level of the information;

c) statistical results related exclusively to public variables shall not be the subject of the threshold rule;

d) the threshold rule may be disregarded if the statistical result does not reasonably allow identifying statistical units in light both of survey type and of the nature of the associated variables;

e) statistical results related to the same population may be disseminated in such a manner as to prevent establishing links between them and/or with other known sources of information that might enable identification;

f) confidentiality shall be assumed to be adequately protected if all the statistical units of a given population show the same modality in respect of a variable.

Chapter II – INFORMATION NOTICES, COMMUNICATION, AND DISSEMINATION

Article 6. Information Notice

1. In collecting data for a statistical purpose, the data subject shall be notified – within the framework of the information referred to in Section 13 of the decree – of the possibility that his/her personal data may be stored and processed for other statistical and/or scientific purposes, which shall be adequately specified – to the extent that this is known – also by having regard to the categories of recipient.

2. In collecting data for a statistical purpose, provision of information to the individual the data are collected from may be deferred in respect of the specific purposes and the mechanisms of the processing for which the data are intended, where this is found to be necessary in order to achieve the objective of the survey – by having regard to the topic and/or the nature of said survey – and the

processing does not concern sensitive and/or judicial data. In these cases, the information provided to data subjects shall be completed directly the reasons for deferring it cease to apply, unless this proves unreasonable and/or entails the use of positively disproportionate means. The entity in charge of the survey shall draw up a document – which shall be kept for three years as of conclusion of the survey and made available to data subjects exercising the rights as per Section 7 of the decree – setting out the specific reasons why provision of the information to data subjects was deferred, the information items that were deferred, and the mechanisms implemented to inform data subjects once the reasons for deferring the information ceased to apply, or else the grounds on which the information in question was withheld.

3. If the objectives of the survey, the nature of the data, and the circumstances of the collection are such – with regard to scientifically reliable parameters – as to allow an entity to be held liable on behalf of another one in its capacity as family member and/or cohabiter, the data subject may be informed by the agency of the respondent, providing the processing does not concern sensitive and/or judicial data.

4. If the data are collected from third parties or the processing for statistical and/or scientific purposes concerns data that have been collected for other purposes, and the provision of information entails a disproportionate effort compared with the right to be protected, the data controller shall ensure publicity of the processing in the following manner:

- by publishing an ad in at least a newspaper with nationwide circulation, or broadcasting a report via a radio and TV company with nationwide reach, as regards processing operations concerning a high number of entities distributed all over the national territory;
- by publishing an ad in a newspaper with regional (provincial) circulation, or broadcasting a report via a radio and TV company with regional (provincial) reach, as regards processing operations concerning a high number of entities distributed over a regional (provincial) area;
- by publishing an ad in information media that are customarily addressed to the relevant data subjects as regards processing operations concerning specific categories that are identified on the basis of particular population features and/or particular training, occupational, or similar conditions.

The data controller shall notify the Garante in advance of the publicity mechanism it has adopted.

5. If the data controller deems it inappropriate to avail itself of the publicity mechanisms referred to in paragraph 4, partly by having regard to the nature of the collected data and/or the processing mechanisms, or else of the expenses to be incurred in connection with the relevant survey, it may decide on implementing suitable publicity mechanisms that shall be notified in advance to the Garante; the latter may always require certain measures and/or precautions to be taken.

Article 7. Consent

1. Processing for statistical and/or scientific purposes may be carried out by a private entity without the data subject’s consent if it does not concern sensitive and/or judicial data and the information notice provided pursuant to Section 13 of the decree contains a section that sets out whether the data are to be disclosed on a mandatory basis or not, specifically detailing the reasons why the data in question are to be provided on a voluntary basis.

Article 8. Data Communication and Dissemination

1. It shall be allowed to disseminate statistical results, also by publishing them, exclusively in aggregated format, or else in a manner preventing data subjects from being identified also based on indirectly identifying data – except where the dissemination concerns public variables.

2. Personal data that are processed for a given statistical purpose may be communicated, after eliminating identification data, to a university, research body or institution, and/or a researcher for other statistical purposes that shall be clearly set out in writing in the relevant request. In drawing up the relevant research project as per Article 3, the requesting entity shall undertake not to process the data for purposes other than those referred to in the said request as well as not to communicate the data further to third parties; additionally, it shall enclose a copy of the communication request with the project. The requested party, being the controller of the initial processing, shall deposit both the communication request and the related project with the respective university, research body or scientific society, which shall be responsible for keeping them under confidentiality conditions for five years as from the planned completion of the research.

3. Should the requesting party declare that the statistical result cannot be achieved otherwise and expressly set out the relevant grounds in the request as per paragraph 2 above, it shall be permitted to also communicate the identification data. The requested party, having evaluated the aforementioned grounds, shall provide the data in compliance with the data relevance and necessity principles. Article 9 hereof shall be left unprejudiced.

4. The provisions referred to in paragraphs 2 and 3 shall also apply to communication and subsequent transfer, even on a temporary basis, of personal data to universities, research bodies or institutions, and/or researchers that are resident either in a EU Member State or in a country affording adequate protection of personal data.

5. If the processing for a given statistical purpose entails transfer of personal data, also on a temporary basis, to a non-EU Member State affording no adequate protection of personal data, said transfer shall be allowed on the basis of safeguards for data subjects' rights that are comparable with those set out herein, to be adduced by the recipient body and/or researcher by means of a contract to be drawn up in accordance with the standards authorised by the Garante pursuant to Section 40 of the decree, also on the proposal of scientific bodies and/or societies.

Article 9. Processing of Sensitive and Judicial Data

1. As a rule, sensitive and/or judicial data processed for statistical and/or scientific purposes shall be anonymous.

2. Where the lawful, specific statistical or scientific purposes aimed at by the processing of sensitive and/or judicial data cannot be achieved without identifying data subjects, also on a temporary basis, the data controller shall take specific measures to keep the identification data separate ever since collection, unless this proves impossible because of the features of the processing or else entails use of clearly disproportionate means.

3. Where the data as per paragraph 1 are contained in lists, registers, and/or databases that are kept with the help of electronic means, they shall be processed by using either encryption techniques or identification codes and/or other solutions that, in the light of the number and type of the processed

data, make said data temporarily unintelligible also to those entities that are authorised to access them and allow identifying data subjects only if this is necessary.

4. Where the entities referred to in Article 2(1) are private bodies, they may process sensitive data for statistical purposes if

a) the data subject has given his/her consent freely on the basis of the items that are required to be included in the information notice;

b) the consent is given in writing. If the sensitive data are collected in such a manner – e.g. telephone interviews, operator-assisted interviews, etc. – as to make it especially burdensome to obtain consent in writing, said consent may be documented in writing on condition that it is given expressly. In this case, the documents related to provision of the information to the data subject as well as to obtaining his/her consent shall be kept by the data controller for three years;

c) the processing has been authorised by the Garante either following a specific request pursuant to Section 26(1) of the Decree or based on a general authorisation applying to certain categories of data controller and/or processing operation that has been issued pursuant to Section 40 of the Decree, also on the proposal of scientific bodies and societies.

5. Processing of judicial data by the entities referred to in Article 2(1) that are private bodies shall only be allowed if it is authorised expressly by the law and/or a provision issued by the Garante in pursuance of Section 27 of the Decree.

6. Where the entities referred to in Article 2(1) are public bodies, they may process sensitive and/or judicial data

a) for scientific purposes, in compliance with Section 22 of the Decree, on condition that they specify and publish the categories of data and operation that are absolutely relevant and necessary by having regard to the purposes sought in the individual cases, and update this information regularly in pursuance of Section 20, paragraphs 2 and 4, of the Decree;

b) for statistical purposes, in compliance with Section 22 of the Decree, providing the conditions referred to in Section 20, paragraphs 2-4, of the Decree are fulfilled.

Article 10. Genetic Data

1. Processing of genetic data shall only be allowed in the cases and according to the arrangements set forth in an ad-hoc authorisation issued by the Garante pursuant to Section 90 of the Decree.

Article 11. Provisions Applying Specifically to Medical, Bio-Medical, and Epidemiological Research

1. Medical, bio-medical, and epidemiological research shall fall within the scope of application of this code to the extent set forth in Article 2(2) hereof.

2. The research referred to in paragraph 1 shall be carried out in compliance with international and Community guidelines and provisions applying to this subject matter, such as the Convention on

Human Rights and Biomedicine of 4 April 1957, as ratified by Act no. 145 of 28 March 2001, Council of Europe's Recommendation No. R(97)5 adopted on 13 February 1997, on the protection of medical data, and the World Medical Association Helsinki Declaration on the principles for medical research involving human subjects.

3. In any research as per paragraph 1, the information notice shall enable data subjects to make a distinction between research activities and health care-related activities.

4. In expressing his/her consent to medical and/or epidemiological surveys, the data subject shall be requested to declare whether he/she is willing to be informed of any unexpected findings made in his/her regard during the research. If so, the data subject shall be informed in accordance with the mechanisms set out in Section 84 of the decree. If consent cannot be requested because of the reasons specified in paragraph 5 below, the aforementioned findings shall be communicated all the same to the data subject, in compliance with Section 84 of the decree, where they are of major importance with a view to safeguarding the data subject's health.

5. In any research as per paragraph 1, the data subject's consent shall not be required if the following conditions are met pursuant to Section 110 of the decree:

a) it is not possible to inform the data subject on ethical grounds – the data subject being unaware of his/her condition – or else on methodological grounds – it being necessary not to inform the data subject about the assumptions underlying the research and/or the circumstance that he/she was selected therefor – or because it is organisationally unfeasible;

b) the research programme has been the subject of a reasoned favourable opinion issued by the competent ethics committee;

c) the processing has been authorised by the Garante also pursuant to Section 40 of the decree, also upon the proposal of relevant scientific bodies and societies.

Article 12. Supervision

1. Universities, research bodies and/or institutions, and scientific societies shall keep the documents related to the research projects that have been submitted as well as to the undertakings endorsed by researchers pursuant to Article 3(1) and (2) and Article 8(2) hereof.

2. The entities referred to in paragraph 1

a) shall ensure that this Code is disseminated among and complied with by any and all entities that, both inside and outside the relevant organisation, are involved for whatever reason in the processing of personal data that is carried out within the framework of the researches, also by taking suitable measures on the basis of the respective by-laws and regulations; and

b) shall notify the Garante of any breaches of the code coming to their knowledge.

CHAPTER III – SECURITY AND RULES OF CONDUCT

Article 13. Data Collection

1. The entities referred to in Article 2(1) shall pay specific attention to both selecting the staff in charge of data collection and setting out organisational and methodological arrangements for the survey, in order to ensure compliance with this code and safeguard data subjects' rights.

2. The staff in charge of collection shall abide by both the provisions laid down herein and the instructions received. In particular, they shall

a) disclose their identities and functions and the purposes of collection, also by means of appropriate documents;

b) provide the information as per Section 13 of the decree and Article 6 hereof as well as such other explanations as can allow data subjects to answer adequately and knowledgeably, and refrain from any conduct that might be regarded as deception and/or undue pressure;

c) not collect personal data from the same data subjects at the same time on behalf of several data controllers, except where expressly authorised to do so;

d) timely rectify mistakes and inaccuracies affecting the information gathered in the course of data collection; and

e) take special care in collecting sensitive and/or judicial data.

Article 14. Data Retention

1. Pursuant to Section 99 of the decree, personal data may be retained for statistical or scientific purposes also for longer than is necessary to achieve the purposes for which they have been collected and/or subsequently processed. In such cases, the identification data may be retained until they are found to be necessary with a view to

a) continuous longitudinal studies;
b) control, quality, and coverage studies;
c) laying down sampling designs and selecting survey units;
d) setting up archives of statistical units and information systems; and
e) other cases in which this is found to be indispensable based on adequate documentation for the purposes to be achieved.

2. In the cases referred to in paragraph 1, the identification data shall be kept separately from any other data so as to allow for different access levels, except where this is found to be impossible on account of the specific features of the processing, or else entails the use of clearly disproportionate means compared with the right to be protected.

Article 15. Security Measures

1. In adopting the security measures applying to data and systems as per Sections 31 and following ones of the decree and the technical specifications contained in Annex B thereto, the controllers of

processing operations performed for statistical purposes shall also take care of access levels to the personal data in the light of both the nature of the data in question and the tasks discharged by the entities involved in the processing.

Article 16. Exercise of Data Subjects' Rights

1. If the rights as per Section 7 of the decree are exercised with regard to data that are processed for statistical and scientific purposes, the data subject may access the archives concerning him or her in order to request that they be updated, rectified and/or supplemented, providing such operations do not prove impossible because of either the nature or the status of the processing or else entail the use of clearly disproportionate means.

2. Should the aforementioned changes produce no significant effects on the statistical results related to the processing, the data processor shall record the changes requested by a data subject in ad-hoc sections and/or registers without amending the data initially entered in the archive.

Article 17. Rules of Conduct

1. Data processors and persons in charge of the processing that can lawfully access the personal data processed for statistical and/or scientific purposes on grounds related to their work and/or research(es) shall also abide by the following provisions:

a) personal data may only be used for the purposes set forth in the research project as per Article 3 hereof;

b) personal data must be kept in such a manner as to prevent their loss, removal and/or any other use that is not compliant with both the laws and the instructions received;

c) non-publicly available personal data and news that become known in the course of performing statistical activities and/or activities that are instrumental thereto may not be disseminated or used in whatever manner for one's own or another's private purposes;

d) any and all activities performed shall be adequately documented;

e) the professional skills related to personal data protection shall be continuously adjusted to methodological and technological evolution;

f) communication and dissemination of statistical results shall be fostered by having regard to the informational requirements of both the scientific community and public opinion in compliance with personal data protection legislation;

g) any and all conduct that is not in line with the rules of conduct set out herein shall be immediately reported to either the data processor or the data controller.

Article 18. Adjustments

1. Compliance of the provisions set out herein with international and/or other instruments adopted in connection with the protection of personal data that are processed for statistical and scientific

research purposes shall be verified regularly also following reports submitted by the signatory parties. This shall be aimed at amending the code as required in order to bring it into line with the aforementioned instruments, or else at issuing a new code of conduct pursuant to Section 12 of the decree if said amendments are such as to produce substantial effects on the regulations contained herein.

Article 19. Entry into Force

1. This Code shall apply as of October 1st, 2004.

A.5 – CODE OF CONDUCT AND PROFESSIONAL PRACTICE APPLYING TO INFORMATION SYSTEMS MANAGED BY PRIVATE ENTITIES WITH REGARD TO CONSUMER CREDIT, RELIABILITY, AND TIMELINESS OF PAYMENTS

Preamble

We, the undersigned private entities, adopt this Code of conduct and professional practice on the assumption that:

1) processing of personal data within the framework of information systems controlled by private entities that are used for the purposes of consumer credit and/or concern reliability and timeliness of payments shall have to be performed by respecting data subjects' rights, fundamental freedoms, and dignity, with particular regard to the right to personal data protection, confidentiality, and personal identity;

2) this code sets forth adequate safeguards and processing mechanisms to protect data subjects' rights, which shall have to be abided by for the purposes of protecting credit and limiting the relevant risks in order to also facilitate access to consumer credit and reduce the risk of excess indebtment by data subjects;

3) adoption of this code is encouraged by the Garante per la protezione dei dati personali within the framework of representative associations for the relevant industry sector in pursuance of Sections 12 and 117 of the Personal Data Protection Code (legislative decree no. 196/2003 of June 30, 2003);

4) whoever uses personal data for the aforementioned purposes shall have to abide by the rules of conduct set out herein as a fundamental prerequisite for the processing to be lawful and fair;

5) industry operators are also required to comply with the safeguards set out in the data protection Code, with particular regard to obtaining consent and other lawfulness preconditions;

6) this code does not apply to the information systems controlled by public bodies, in particular it does not apply to the centralised risk service managed by Banca d'Italia (as per Sections 13, 53(1), letter b), 60(1), 64, 67(1), letter b), 106, 107, 144, and 145 of legislative decree no. 385 of September 1, 1993, being the Consolidated Statute on Banking and Credit; the CICR's resolution of March 29, 1994; the Banca d'Italia's provision of August 10, 1995; and the Banca d'Italia's circular letter of February 11, 1991 as subsequently updated). The centralised system for low-level risk assessment set up under CICR's resolution of May 3, 1999 as published in the Official Journal no. 158 of July 8, 1999 shall be regulated by some principles set forth herein concerning the provision of information to data subjects and exercise of data subjects' rights insofar as they are compatible with the specifically applicable provisions (see, in particular, Banca d'Italia instructions as published in the Official Journal no. 272 of November 21, 2000).

Article 1

Definitions

1. For the purposes of this code of conduct and professional practice, the definitions listed in the Personal Data Protection Code (hereinafter referred to as the "Code") shall apply (see Section 4 of legislative decree no. 196/2003). For the same purposes, moreover,

a) "credit application/relationship" shall mean any application or relationship concerning the granting of credit in the exercise of commercial and/or professional activities, in the form of a payment extension, a loan, or any other similar financial support as per the Consolidated Statute on Banking and Credit (legislative decree no. 385 of September 1, 1995);

b) "remedying of defaults" shall mean to extinguish the defaults on money obligations due either to defaults on payments or payment delays without losses and/or balance receivables also in the form of interests and charges, as well as to extinguish said obligations by means other than the relevant performance, in particular following settlement and/or composition;

c) "credit information system" shall mean any database concerning credit applications/relationships that is managed in a centralised fashion by a legal person, an organisation, an association and/or another private body and can only be accessed by the entities communicating the information recorded therein and participating in the relevant information system. The system may contain, in particular,

1) negative credit information, only concerning credit relationships affected by defaults;

2) positive and negative credit information concerning credit applications/relationships irrespective of the existence of defaults as recorded in the system at the time they occurred;

d) "manager" shall mean any private entity acting as controller of the processing of the personal data recorded in a credit information system and managing said system by setting out the mechanisms applying to its operation and use;

e) "participant" shall mean any private entity that acts as a controller of the processing of the personal data that are collected in connection with credit applications/relationships, participates in the relevant credit information system based on an agreement and/or contract with the manager, and can use the data contained in the system, being under the obligation to notify the manager systematically of said personal data as related to credit applications/relationships within the framework of mutual data exchanges with other participants. Except for the entities providing credit-factoring services, a participant may be

1) a bank,

2) a financial broker,

3) any other private entity that, in the exercise of commercial and/or professional activities, grants an extension for the payment related to the supply of goods and/or services;

f) “consumer” shall mean a natural person who, in connection with a credit application/relationship, acts for purposes that cannot be related to his/her professional and/or business activity, if any;

g) “data retention period” shall mean the period during which the personal data related to credit applications/relationships are retained in a credit information system and can be used by participants for the purposes referred to in this code;

h) “automated credit scoring techniques and/or systems” shall mean the mechanisms to organise, aggregate, compare and/or process personal data related to credit applications/relationships as consisting in the use of automated systems based on statistical methods or models with a view to assessing credit risk, whose results are expressed in the form of summary judgments, figures and/or a score that is/are associated with a given data subject and aim at providing the predictive and/or probability-based description of said data subject’s risk profile, reliability and/or timeliness of payment.

Article 2

Purposes of the Processing

1. The personal data contained in a credit information system may only be processed by the manager and participants for the purpose of protecting credit and limiting the relevant risks, and in particular, to assess data subjects’ financial status and creditworthiness or anyhow their reliability and timeliness of payment.

2. No other purposes may be pursued, especially in connection with market surveys and/or the promotion, advertising and/or direct selling of products or services.

Article 3

Data Quality and Categories

1. Processing within the framework of a credit information system may only concern data related to the entity that either applies for or is a party to a credit relationship with a participant as well as the data related to any surety, including a joint surety, whose position is clearly separate from that of the principal debtor.

2. Processing may not concern sensitive or judicial data, and shall concern objective personal data that are closely relevant and not excessive in respect of the purposes sought and relate to a credit application/relationship as well as to any event occurring on whatever ground and for whatever purpose until remedying of the relevant defaults in compliance with the retention periods set out in Article 6.

3. The following data categories may be processed in connection with each credit application/relationship reported to a credit information system, and said categories shall have to be

specified by the manager in a list that is to be made easily available on the manager's own website on the communications network as well as being communicated in detail to any data subject that so requests:

a) census register data, taxation ID, and/or VAT register number;

b) data related to the credit application/relationship concerning, in particular, the type of contract, the amount of credit, the repayment mechanisms, and the status of the application and/or contract performance;

c) accounting data related to payments, time pattern of payments, indebtment including residual debt, and condensed information on accounting status of the given relationship;

d) data related to credit factoring and/or litigations, assignment of credit, and/or exceptional events affecting assets and liabilities and/or status of corporations, legal persons and/or other entities.

4. Any and all codes and criteria used to record the data in a credit information system and to facilitate their processing shall only be aimed at providing the objective, accurate representation of said data as well as of any events occurring in connection with the relevant credit relationship. The aforementioned criteria and codes shall be used in conjunction with detailed information as to their meaning, to be provided by the manager, complied with by participants, and made easily available by both, also at the data subjects' request.

5. The identification data concerning the participant that has communicated the personal data related to a credit application/relationship shall be recorded in the credit information system. Said identification data shall be accessible to both the manager and the data subjects, whilst they may not be accessed by other participants.

Article 4

Data Collection and Recording

1. Subject to the provisions made in paragraph 5, a manager shall acquire the personal data to be recorded in the credit information system exclusively from participants.

2. Each participant shall take appropriate measures to verify and ensure that the data communicated to the manager may be lawfully used in the system and are accurate and fair.

3. Upon receiving the data, the manager shall verify their congruence by means of logic and formal controls; if the data are found to be incomplete and/or incongruous, the manager shall send them back to the participant that has communicated them for the necessary amendments and/or additions to be made. After performing said controls and such amendments or additions as may be necessary, the data shall be recorded in the credit information system and made available to all participants.

4. Each participant shall carefully verify the data it processes and comply promptly with any verification requests made by a manager, also following exercise of a right by data subjects.

5. Any data recorded in a credit information system shall be deleted, supplemented and/or amended either directly by the participant that has communicated said data, where this is technically feasible,

or by the manager at the request of or else in agreement with the relevant participant, also following exercise of a right by data subjects, or in pursuance of an order issued by judicial authorities and/or the Garante.

6. The data related to the first payment delay in a credit relationship shall be used and made available to other participants in compliance with the terms below:

a) in negative credit information systems, after at least one hundred and twenty days as of the relevant payment deadline, or in case the debtor defaulted on at least four monthly instalments and these were not remedied;

b) in positive and negative credit information systems,

1) if the data subject is a consumer, after sixty days of the monthly update referred to in paragraph 8, or in case he/she defaulted on at least two consecutive monthly instalments, or if the delay has to do with either the last or the last but one instalment. In the second case referred to above, the data shall be made available after the monthly update concerning the second consecutive default;

2) in all other cases, after at least thirty days following the monthly update referred to in paragraph 8, or in case the debtor defaults on one instalment.

7. In case of payment delays, the participant shall inform the data subject, also at the time reminders or other notices are sent, that his/her data will be shortly recorded in one or more credit information systems. The data concerning the first delay as per paragraph 6 may be made available to participants after at least fifteen days as of sending the aforementioned information to the data subject.

8. Subject to the provisions made in paragraph 6, the data recorded in a credit information system shall be updated regularly at monthly intervals by the participant that has communicated them.

Article 5

Information Notice

1. At the time of collecting the personal data related to credit applications/relationships, a participant shall inform the data subject pursuant to Section 13 of the Code also with regard to the processing of personal data that is performed within the framework of a credit information system.

2. The information referred to in paragraph 1 shall include clear-cut, accurate details concerning, within the framework of the description of the purposes and mechanisms of the processing as well as of the other elements referred to in Section 13 of the Code,

a) identification data concerning both the credit information systems the personal data are communicated to and the respective managers;

b) the categories of participant accessing said systems;

c) the data retention periods in the credit information systems such data are communicated to;

d) arrangements applying to organisation, comparison and processing of the data and the use, if any, of automated credit scoring techniques and/or systems;

e) mechanisms for data subjects to exercise the rights referred to in Section 7 of the Code.

3. The information referred to in paragraph 2 shall be provided to data subjects in writing according to the model notice that is attached to the decision whereby compliance of this code with the law is certified. If the information notice is included in a form used by the participant, it shall be appropriately highlighted and placed as a separate, unified item within sections and/or boxes other than those related to different purposes of the processing carried out by said participant.

4. The information to be provided on account of updates and/or changes concerning the data pursuant to paragraph 2 shall be made available via regular communications as well as on one or more Internet web sites and/or if a data subject so requests, also with regard to changes in the manager's registered office and/or name.

5. More detailed information shall be provided by the manager via additional dissemination mechanisms, including the use of electronic networks, to supplement the information notice provided by participants to the individual data subjects.

6. If the credit application is not granted, the participant shall inform the data subject as to whether it has consulted personal data related to negative credit information in one or more systems with a view to dealing with the credit application, and it shall provide said data subject with the details required to identify both the system used as the source of the information and the respective manager.

7. The participant shall provide the data subject with the additional information referred to in Articles 9(1), letter d), and 10(1), letter c).

Article 6

Data Retention and Updating

1. The personal data related to credit applications as communicated by participants may be retained in a credit information system for as long as necessary in order to deal with said applications and at all events for no longer than one hundred and eighty days as of the date of submission of the aforementioned applications. If the credit application is not granted, or if it is waived, the participant shall inform the manager thereof in connection with the monthly update referred to in Article 4(8). In the latter case, the personal data related to the application that has been waived by the data subject and/or rejected may be retained in the system for no longer than thirty days as of their update.

2. Negative credit information related to payment delays that are subsequently remedied may be retained in a credit information system

a) for up to twelve months as of the recording of the data concerning remedying of delays not in excess of two instalments/two months; or

b) for up to twenty-four months as of the recording of the data concerning remedying of delays in excess of two instalments/two months.

3. Upon expiry of the terms referred to in paragraph 2, the data shall be removed from the credit information system if no data concerning further delays and/or defaults is recorded during said terms.

4. Participant and manager shall promptly update the data concerning remedying of defaults of which they are aware, where such remedying takes place after the participant's assignment of its credit to an entity that does not participate in the relevant system, also if the data subject so requests by submitting either a statement rendered by the credit assignee or any other suitable instrument.

5. Negative credit information related to defaults that are not subsequently remedied may be retained in a credit information system for no longer than thirty-six months as of the expiry of the relevant contractual agreement; if other events occur that are material to the payment, said information may be retained for no longer than thirty-six months as of the date on which the information had last to be updated or the relevant relationship was terminated.

6. Positive credit information related to a relationship that was concluded by extinguishing all monetary obligations may be retained in a system for no longer than twenty-four months as of the date of termination and/or expiry of the relevant contractual agreement, or else as of the first update performed in the month following the aforementioned dates. In light of the requirement whereby the data should be complete in respect of the purposes to be achieved (see Section 11(1), letter d), of the Code), the aforementioned positive credit information may be retained further in the system if the latter contains negative credit information related to delays and/or defaults that have not been remedied with regard to other credit relationships concerning the same data subject. In the latter case, the positive credit information shall be removed from the system upon expiry of the term set out in paragraph 5 as to retention of the negative information recorded in the system in respect of any other credit relationships concerning said data subject.

7. If the consumer concerned notifies a participant that he/she is withdrawing his/her consent to the processing of positive information within the framework of a credit information system, the participant shall inform the manager thereof in connection with the monthly update referred to in Article 4(8). In the latter case as well as in case withdrawal of consent is communicated directly by a data subject, the manager shall record this news in the system and remove the information by no later than ninety days as of said update and/or communication.

8. Prior to removing the data from a credit information system in accordance with the specifications set out in the above paragraphs, a manager may transfer the data to another medium in order to retain them exclusively for as long as necessary with a view to defending a legal claim, or else in order to process the data in anonymous format for statistical purposes.

9. The provisions of this Article shall not apply to retention by a participant, for internal use, of contractual and/or accounting records containing the personal data related to a credit application/relationship.

Article 7

Use of Data

1. A participant may access a credit information system also by consulting a copy of the respective database with regard to data that fall justifiably within its scope of interest and may only concern:

a) consumers that apply for and/or are parties to a credit relationship with said participant as well as any surety, including joint sureties,

b) entities acting in the context of their business and/or professional activities, in respect of which investigations have been started in order to set up a credit relationship or undertake a credit risk, as well as entities that are already parties to a credit relationship with said participant,

c) entities that are legally related to those referred to in letter b) above, in particular because they act as joint sureties or else belong to corporate groups, providing the personal data to be accessed by the participant are factually necessary in order to assess financial status and creditworthiness of the entities referred to in said letter b).

2. A credit information system may be accessed by a participant and/or a manager exclusively via a limited number of data processors and persons in charge of the processing, to be specified in writing, as well as by having regard only to such data as are absolutely necessary, relevant and not excessive in respect of the purposes set out in Article 2, in connection with the specific requirements resulting either from the investigations performed following a credit application or from the management of a credit relationship, which must be verifiable in concrete on the basis of the information available to said participant(s). The system may also be accessed by banks and financial brokers that are members of the participant's banking group in compliance with the aforementioned limitations and mechanisms, exclusively with a view to dealing with the investigations required either to set up a credit relationship with the relevant data subject or anyhow to undertake the relevant risk.

3. Participants shall access the credit information system via the mechanisms and tools, including electronic tools, that have been set out in writing jointly with the manager in compliance with personal data protection legislation. The personal data related to credit applications/relationships recorded in a credit information system may be consulted via stepwise, selective access mechanisms that shall envisage one or more consultation levels providing summary and/or condensed information in respect of the data subject prior to allowing access to detailed information, which shall also apply to the data concerning sureties and/or related entities as per paragraph 1. It shall not be feasible, also from a technical standpoint, to access the data in a manner allowing bulk queries and/or acquisition of lists of data regarding credit applications/relationships in respect of entities other than those applying for and/or participating in a credit relationship with the relevant participant.

4. Furthermore, it shall not be allowed for third parties to access a credit information system except for the requests made by judicial and police authorities for purposes of justice, or else by other public institutions, authorities, administrative agencies and bodies exclusively in the cases referred to in laws, regulations and/or Community legislation as well as in compliance with the relevant provisions.

Article 8

Access and Exercise of Other Rights by Data Subjects

1. With regard to the personal data recorded in a credit information system, data subjects shall be entitled to exercise their rights in accordance with the mechanisms set out in the Code both in respect of the manager and in respect of the participants that have communicated said data. The latter entities shall be responsible for dealing promptly and in full with the relevant requests, also by taking suitable organisational and technical measures.

2. In the request made to exercise his/her rights, a data subject shall also specify, if possible, his/her taxation ID and/or VAT Register number in order to facilitate searching the data concerning him/her in the credit information system.

3. Any third party that is empowered by the data subject in writing to act as an attorney or delegated entity in order to exercise the relevant rights may only process the personal data acquired from a credit information system for the purpose of protecting the data subject's rights, any other purpose sought by said third party and/or entities related to the latter being ruled out.

4. Any participant receiving a request whereby any of the rights referred to in Section 7 of the Code is exercised in respect of the credit information recorded in a system shall answer directly under the terms set out in Section 146(2) and (3) of the Code and shall have the data amended as required in pursuance of Article 4(5). If the request is lodged with the manager, the latter shall also answer directly under the same terms and consult with the participant if necessary.

5. Where it is necessary to carry out additional and/or specific controls with the participant, the manager shall inform the data subject thereof within the fifteen-day term provided for in the Code and set another term for the relevant answer, which may not be in excess of fifteen additional days. During the period required to carry out the additional controls with the participant, the manager:

a) shall keep track of the performance of the aforementioned controls in the credit information system throughout the initial fifteen-day term, by means of a specific code and/or an ad-hoc message to be posted with the data that are the subject of the request made by the data subject, and

b) shall suspend display of the data that are being controlled in the credit information system throughout the additional fifteen-day term.

6. If the request referred to in paragraph 4 concerns a complaint for non-performance against the seller/provider of the goods or services that are the subject of the contract underlying the credit relationship, the manager shall promptly record a notice to that effect in the credit information system at the request of either the data subject or the participant, or else by informing the latter, via a specific code to be posted with the data related to the credit relationship in question.

Article 9

Use of Automated Credit Scoring Techniques and Systems

1. Where the personal data contained in a credit information system are also processed by means of automated credit scoring techniques and systems, the manager and participants shall be responsible for ensuring compliance with the following principles:

a) the techniques or systems made available by the manager, or else implemented on the participants' behalf, may only be used for investigating a credit application and/or managing the credit relationships already set up;

b) the data concerning judgments, markers and/or scoring associated with a given data subject shall be processed and communicated by the manager only to the participant that either has received the relevant credit application from the data subject or previously communicated data related to the relevant credit application; at all events, the data may not be retained in the credit information system pursuant to Article 6 of this code, nor may they be made available to the other participants;

c) statistical models and/or factors as well as the algorhythms used to calculate judgments, markers and/or scoring shall be verified regularly at least on an annual basis and updated as a function of the outcome of said verification;

d) where a credit application is not granted, the participant shall inform the data subject as to whether it has consulted data related to negative judgments, markers and/or scoring that have been obtained by means of automated credit scoring techniques and systems, in order to investigate said credit application; if the data subject so requests, the participant shall provide him or her with the data in question and explain both the logic underlying operation of the systems implemented and the main factors that have been taken into account in processing the application.

Article 10

Processing Data from Public Sources

1. If the manager of a credit information system processes, whether directly or by the agency of subsidiary and/or related companies, personal data from public registers, lists, records or publicly available documents, in whatever manner, or if it provides participants with services to access the data from said sources, manager and participants shall be responsible for ensuring compliance with the principles reported below subject to the limitations and arrangements set out in the law as for availability and publicity of the data in question as well as to the provisions referred to in Section 61(1) of the Code:

a) the personal data from public registers, lists, records or publicly available documents, if recorded, must be contained in personal data banks that are separate from and not connected with the credit information system;

b) if a participant accesses personal data contained both in a credit information system and in any of the data banks referred to in letter a), the manager shall take suitable technical and organisational measures to ensure that the data from the credit information system can be separated and distinguished from those originating from other data banks, also by adding appropriate notices, so as to do away with any and all ambiguities as to the different nature and sources of the accessed data;

c) if a credit application is not granted, the participant shall inform the data subject as to whether it has also consulted negative data contained in the data banks as per letter a) in order to investigate the credit application, and it shall specify the public source(s) of said data at the data subject's request.

Article 11

Data Security Measures

1. Any personal data that is processed within the framework of a credit information system shall be confidential information and may not be disclosed to third parties except for the cases envisaged both in the Code and in the above articles.

2. The natural persons that have been appointed by either the manager or the participants as data processors or persons in charge of the processing may access the credit information system, shall keep confidential the personal data acquired, and shall be liable for any breach of confidentiality resulting from use of the data and/or disclosure of the data to third parties for purposes other than or incompatible with those referred to in article 2 hereof, or anyhow for unlawful purposes.

3. Manager and participants shall take suitable technical, logical, informational, procedural, physical, and organisational measures to ensure security, integrity, and confidentiality of personal data and electronic communications in line with personal data protection legislation.

4. The manager shall take adequate security measures to ensure proper functioning of the credit information system as well as access control. Accesses shall be recorded and stored in the information system by the manager as well as by all participants in the possession of a copy of the relevant database.

5. As for compliance with the security, confidentiality, and secrecy obligations referred to herein, manager and participants shall issue specific instructions in writing to the respective data processors and persons in charge of the processing and shall ensure that said instructions are fully abided by also by means of verifications carried out by suitable supervisory bodies.

Article 12

Sanctions

1. Without prejudice to such sanctions as are provided for by the administrative, civil, and criminal laws in force, managers and participants shall jointly lay down, also by the agency of the associations underwriting this code, suitable mechanisms to impose sanctions that are proportionate to the seriousness of the relevant breaches, in particular as regards the trade associations underwriting this code as well as the body referred to in Article 13(7), after informing the Garante thereof. Such measures shall include an official warning, suspension or withdrawal of the authorisation to access the credit information system, and – in the most serious cases – publication of the news concerning the breach(es) in one or more dailies or magazines with nationwide circulation at the offender’s expense.

Article 13

Transitional and Final Provisions

1. The measures required to implement this code of conduct and professional practice shall be adopted by the entities required to abide by it within and no later than April 30, 2005.

2. Within the term set out in paragraph 1, the manager of the centralised system for low-level risk assessment as set up by CICR's resolution of May 3, 1999 (published in the Official Journal no. 158 of July 8, 1999) as well as the respective participants shall take the necessary measures to implement Articles 5 and 8, paragraphs 1, 2, 3, 4, and 5, first sentence, of this code concerning provision of an information notice to data subjects and exercise of rights, which shall supplement the requirements laid down in point 3 of the Banca d'Italia's instructions (published in the Official Journal no. 272 of November 21, 2000).

3. Within three months as of the term referred to in paragraph 1, participants shall provide the information referred to in Article 5(1) and (2) of this code in the context of the regular communications sent to customers, where said information is not included in the information notices previously made available to any data subject whose personal data are already recorded in a credit information system

4. In the initial implementing phase of the provisions referred to in Article 6(6), managers shall reduce the retention period of personal data related to positive credit information to no longer than thirty-six months, by June 30, 2005. The body referred to in Article 7 shall evaluate, by means of a reasoned instrument, whether the experience gathered up to that time and the impact of the measures envisaged in this code on data subjects' rights are such as to justify the continued application of the said thirty-six month term. The latter shall be regarded as applicable further unless the Garante provides otherwise either at the request of said body or of its own motion. By January 31, 2006, the Garante shall order publication in the Official Journal either of its own provision or of a notice specifying the term to be complied with.

5. In order to allow verifying implementation of the provisions set out in this code, each manager shall provide the Garante, by no later than two months as of expiry of the term referred to in paragraph 1, in accordance with the arrangements referred to therein,

a) with a general description of the operation of the credit information system and the mechanisms for the participants' access thereto, in addition to its own identification data and contact details, so as to allow assessing adequacy of the measures, including technical and organisational measures, that have been taken to implement this code;

b) with the model contracts, agreements, conventions, regulations and/or instructions applying to participants' participation in and access to the credit information system, as regards the components that are relevant to personal data protection and the implementation of this code, as well as with the documentation concerning the measures that have been taken regarding data security, confidentiality, and secrecy;

c) with the documents referred to in Articles 3(3) and (4), 5(4) and (5), and in paragraph 7 below.

6. The communications referred to in paragraph 4 shall be sent to the Garante, also after expiry of the aforementioned term, by any data controller acting in the capacity as manager of a credit information system where said data controller intends to proceed with the processing of personal

data falling under the scope of application of this code. Managers shall notify the Garante of any changes in previously sent communications and documents by no later than the end of the year in which said changes took place.

7. The manager shall regularly verify, at least at yearly intervals, that the processing is lawful and fair by checking that the data related to a suitable number of credit applications/relationships selected on a sample basis are accurate and complete. Said controls shall be carried out by a body including at least a representative from the manager, a representative from the participants to be appointed on a rotational basis, and a representative from consumer associations to be appointed by the National Consumers' and Users' Council. The minutes of the aforementioned controls shall be transmitted to the Garante.

8. In order to supervise over compliance with the provisions set out herein, subject to the powers provided for by the Code concerning investigations and controls, the Garante may agree with the manager on performance of additional regular verifications at the premises where the personal data are processed, including accesses – also on a sample basis – to the credit information system. The Garante may carry out similar verifications to be agreed upon jointly in respect of the accesses by participants.

9. The trade associations undersigning this code as well as the managers shall start co-operation initiatives with consumer associations and the Garante in order to devise both operational solutions to foster compliance with this code and alternative mechanisms to solve any disputes resulting from the application of this code.

10. The Garante shall encourage regular reviews and upgrades of this code in the light of technological developments, the experience gathered in its application, and regulatory changes, also if so requested by the trade associations undersigning this code.

Article 14

Entry into Force

1. This code shall apply as of January 1, 2005.

A.6 – CODE OF PRACTICE APPLYING TO THE PROCESSING OF PERSONAL DATA PERFORMED WITH A VIEW TO DEFENCE INVESTIGATIONS

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Code of Practice Applying to the Processing of Personal Data Performed with a View to Defence Investigations

Foreword

We, the entities mentioned hereinafter, undersign this Code of practice on the basis of the following assumptions:

1. Several entities, in particular lawyers and trainee-lawyers included in the respective registers and professional rolls as well as the entities carrying out authorised private detective activities in pursuance of the law, make use of personal data to perform defence investigations in connection with criminal proceedings (under Act no. 397 dated 7 December 2000), or else in order to establish or defend a judicial claim. Use of such data is indispensable to ensure full, effective protection of the rights in question, with particular regard to the right of defence and the right to evidence; effective protection of both rights is not jeopardised, in fact it is enhanced, by the principle whereby personal data must be processed in compliance with the rights, fundamental freedoms and dignity of data subjects as related, in particular, to confidentiality, personal identity, and the right to personal data protection (see sections 1 and 2 of the DP Code);
2. Such specific adjustments and/or precautions as may be provided for by law and/or this code of practice may not be applicable if the data are processed for purposes other than those laid down in article 1 of this code;
3. Being aware of the paramount importance to be attached to the legitimate exercise of the right of defence and the protection of professional secrecy, we, the aforementioned entities, consider it necessary to take account of specific features of our professional activities with particular regard to sensitive and/or judicial personal information. This is aimed at highlighting the peculiarities inherent in looking up, collecting, using and storing data, statements and documents for defence purposes, in particular as related to judicial proceedings, as well as at preventing such implementing uncertainties as have arisen from time to time and have led ultimately to envisage useless safeguards that are not provided for in any items of legislation – in fact, they are at times in conflict with standard operational requirements. The paramount interest in the legitimate exercise of the right of defence must be respected in all cases, including inspection activities; additionally, account must also be taken of the constraints placed by law on the exercise of data subjects' rights (section 7-9 of the DP Code) with a view to safeguarding the right of defence;
4. Data processing for defence purposes contributes to a professional's standing training and gives rise to a set of legal practice precedents that has lasting significance – possibly to meet defence requirements – well after expiry of the retainer and represents an instance of that professional's activity as well;
5. Legislation and implementing instruments already set forth safeguards and arrangements to be complied with in order to protect the personal data that are processed to establish or defend a judicial claim and/or to carry out defence investigations. The safeguards in question – which do not apply to anonymous data – have already allowed clarifying, for instance, under what conditions personal data may be collected without the person's consent and without providing specific information, and that those data may be used for defence

a. the information notice to be given to data subjects, which may fail to include any items that are already known to the data subject and may be worded concisely and informally as appropriate by taking account of the trust relationship established with one's customer and/or of the specific professional task; the information may also be provided only verbally and once and for all by having regard to all the data collected whether from the data subject or from third parties. It is permitted not to provide the information notice in respect of the data collected from third parties if such data are processed exclusively for as long as may be necessary to establish or defend a judicial claim or else for the purpose of defence investigations; it should be considered that a data is not collected from the data subject if it results from a lawful remote monitoring activity, in particular where such monitoring does not entail any direct interaction with the data subject (see section 13(5)b. of the DP Code);
b. the consent to be obtained from data subjects, which is not required if the processing is necessary to comply with legal obligations and/or the data at issue – including sensitive data – are processed for defending a right also by means of defence investigations. This applies to the data that are processed in the course of a proceeding – including administrative, arbitration and/or conciliation proceedings –, the data processed in the preparatory phase prior to possibly instituting a proceeding – also in order to check whether the right at issue can be actually defended in court – and the data processed after the dispute is settled whether in or out of court. If the data are suitable for disclosing health or sex life, it is necessary to abide by the principle whereby such data may be processed if the right to be protected – irrespective of whether it arises from unlawful activities or events – is not "overridden by the data subject's right, or else if it consists in a personal right or any other fundamental, inviolable right or freedom" (section 24(1)f. and section 26(4)c. of the DP Code; see general authorisations no. 2/2008, 4/2008 and 6/2008, and the DPA's decision dated 9 July 2003);
c. the right to access one's personal data and exercise any other rights vested in data subjects as for the processing of those data, which may be postponed under the law for as long as such exercise might be specifically and tangibly prejudicial to the performance of defence investigations and/or the establishment of judicial claims (see section 8(2)e. of the DP Code);
d. cross-border transfers of the data where performed exclusively for the purposes of defence investigations or anyhow in order to establish or defend a judicial claim; such transfers, providing they are performed for no longer than is absolutely necessary, are not prohibited whether they are targeted to EU or non-EU countries (see sections 42 and 43(1)e. of the DP Code);
e. notification of the processing, which is not required in respect of many processing operations performed to establish or defend a judicial claim and/or to carry out defence investigations (see section 37(1) of the DP Code, and the DPA's decision no. 1 dated 31 March 2004 including the explanatory note no. 9564/33365 dated 23 April 2004);
f. appointment of persons in charge of the processing and data processors, if any, taking account that one is allowed to avail himself/herself of entities that can lawfully process the data at issue (colleagues, collaborators, partners, process agents, alternates, experts, and consultants not acting in their capacity as data controllers: see sections 29 and 30 of the DP Code);

g. specific data categories such as genetic data, which are already covered by certain safeguards with particular regard to compliance with proportionality requirements, security measures, information notices to data subjects and provision of consent (section 90 of the DP Code; see the DPA's general authorisation dated 22 February 2007);
h. law informatics as per sections 51 and 52 of the DP Code, which is the subject of ad-hoc legal provisions setting out the appropriate precautions in order to protect data subjects without jeopardising scientific and legal information;
i. use of public data and any other information contained in public registers, lists, instruments and/or publicly available documents or else in databases, archives and registers including the registry of births, marriages and deaths, whereby personal information may be retrieved lawfully from such sources and reported in certificates and statements that can be used for defence purposes;

6. Given the above scenario, this Code sets forth supplementary rules of conduct that make up an essential precondition for the data to be processed both fairly and lawfully – even though they produce no direct effects on disciplinary breaches. The Code in question is without prejudice to the rules of professional practice and/or the decisions made in this connection by the competent sector-related bodies, which remain enforceable as a separate, autonomous set of determinations – in particular as for the Code of Practice of the Bar. On the other hand, non-compliance with the latter Code may be relevant with a view to assessing lawfulness and fairness in the processing of personal data;
7. Data protection is supported by additional principles that are already enshrined in the Criminal Procedure Code as well as in the Code of Practice of the Bar – in particular as for confidentiality and secrecy obligations also vis-à-vis former clients; the disclosure of information that is confidential and/or subject to professional secrecy; disclosure of clients' names; recording of conversations between lawyers; and correspondence between colleagues. Other rules of conduct set forth by the Union of Italy's Criminal Lawyers and/or other signatory bodies of this Code are also helpful in this regard.

Chapter I – General Principles

Article 1 – Scope

1. The provisions of this code must be complied with by the following entities in processing personal data to carry out defence investigations and/or to establish or defend a judicial claim whether during a proceeding – including administrative, arbitration and conciliation proceedings – or in the preparatory phase prior to instituting a proceeding, or else upon conclusion of a proceeding:
    a. Lawyers and/or trainee lawyers included in district rolls and/or the relevant registers, sections and lists whether working alone or as a law firm or partnership and providing in-court and out-of-court assistance and/or advisory services, whether based on a retainer or not, also by means of collaborators and employees; foreign lawyers practising in the State's territory in compliance with the law;
    b. Entities carrying out private investigation activities also when hired by defence counsel (see general authorisation no. 6/2007, point 2) – under the terms of section 134 of Royal decree no. 773 dated 18 June 1931 and section 222 of the co-ordination provisions applying to the Criminal Procedure Code.

2. The provisions set forth in this Code shall also apply to any entity processing personal data for the purposes mentioned in paragraph 1, in particular to any other self-employed

professionals and/or any other entities providing assistance and/or advisory services for the same purposes in compliance with the law, based on an ad-hoc appointment.

Chapter II – Processing Operations by Lawyers

Article 2 – Processing Arrangements

1. A lawyer shall make such arrangements in processing personal data, also without automated means, as are found to be appropriate, on a case by case basis, to foster actual respect for data subjects' rights, freedoms and dignity; in so doing, the purpose limitation, data minimization, and non-excessiveness principles shall have to be applied, the envisaged safeguards shall have to be assessed as to their substance rather than their form, and the quality and amount of the information to be processed shall have to be taken into account along with the possible risks.

2. Any decisions on the issues mentioned in paragraph 1 shall be made by the data controller, who shall consist – depending on the specific circumstances – in
    a. The given professional;
    b. Several professionals whether acting as joint defence counsel for the same client or involved in the relevant professional activity in their capacity as advisors and/or service agents, also without being appointed as defence counsel;
    c. An association or partnership among professionals.

3. Within the framework of the appropriate instructions to be given in writing to the persons in charge of the processing, who must be appointed, as well as to the data processors, who may be appointed on an optional basis (see sections 29 and 30 of the DP code), specific guidance shall be provided on the arrangements to be complied with by the said entities; account shall be taken in this connection of the role vested in each entity - i.e. as a deputy barrister, practising or non-practising trainee lawyer, party-appointed expert, court-appointed expert, private detective and/or as an entity not acting in their capacity as separate data controllers, or else as a trainee, intern, or person in charge for administrative collaboration.

4. Specific attention shall be paid to the adoption of suitable precautions to prevent data from being collected, used or disclosed without justification if
    a. Highly confidential items of information, data and/or documents are acquired, including where such information, data and documents may entail specific risks to data subjects;
    b. Correspondence is exchanged, in particular via electronic networks;
    c. Professionals in a law firm carry out activities in respect of their own client portfolio;
    d. Any data is used whose lawfulness is questionable, partly because of the use of invasive techniques;
    e. Data contained in specific devices and/or media, in particular electronic media (including audiovisual recordings), and/or in specific documents (telephone and Internet traffic data records, technical and experts' reports, reports by private detectives) are used and destroyed;
    f. Records are kept but not used in a proceeding, and database queries are performed for internal purposes, in particular if those databases can be accessed also via electronic networks from offices of the same data controller that are located elsewhere;
    g. Data and/or documents are acquired from third parties after checking that one has the right to obtain such data and documents;
    h. Records are kept that relate to cases already dealt with.

5. If a data is processed to exercise the right of defence before a judicial authority, this may take place prior to instituting the relevant proceeding on condition the data in question is strictly functional to exercising the right of defence and the principles of proportionality, relevance, completeness and non-excessiveness are complied with by having regard to the defence purposes (see section 11 of the DP Code).
6. The following data are used lawfully and fairly:
    a. The personal data contained in public registers, lists, rolls, records or publicly available documents as well as in databases, archives and lists including the register of births, marriages and deaths; personal information may be lawfully retrieved from the said repositories and reported in certifications and statements that may be used for defence purposes;
    b. Records, notes, statements and information acquired in connection with defence investigations, in particular under sections 391-bis, 391-ter and 391-quater of the Criminal Procedure Code, whereby any requests for copies thereof shall not be granted without justification. Should it happen that any data is collected that is excessive and irrelevant vis-à-vis the defence purposes, also when acquiring statements and information in pursuance of the said sections 391-bis, 391-ter and 391-quater of the Criminal Procedure Code, that data shall belong with any other data collected as above if it cannot be extracted and/or destroyed.

Article 3 – Single Information Notice

1. A lawyer may provide an information notice on the processing of personal data (under section 13 of the DP Code) in one with the information he/she is required to disclose in pursuance of defence investigation legislation – e.g. by posting them in the premises of the law firm and/or on the respective website, where available; the information may also be worded concisely and informally.

Article 4 – Data Retention and Erasure

1. The fact that a proceeding pending before a judicial authority is concluded and/or the given assignment has been fulfilled does not entail that the data are to be disposed of. Once the proceeding is extinguished and/or the relevant retainer expires, any records and/or documents concerning the subject matter of the defence and/or defence investigations may be kept – either as originals or in copies – also in electronic format, if this is found to be necessary by having regard to foreseeable, additional defence requirements applying to the relevant client and/or data controller. This is without prejudice to use of the data in question in anonymous format for scientific purposes. The relevant assessment shall be carried out by having regard to the type of data. Where the data are to be retained to comply with legal obligations including taxation and the fight against crime, only such personal data as is actually necessary to comply with the said obligations shall be retained.
2. Without prejudice to the provisions set forth in the Code of Practice of the Bar as for returning the original documents to one's client, and unless provided otherwise by the law, it shall be allowed to destroy, erase or deliver the full documents contained in past case files and the respective copies to the person entitled thereto and/or to the latter's heirs and assigns, on condition the relevant client is notified thereof beforehand.
3. Should the power of attorney and/or the retainer be withdrawn or waived, such documents as have been acquired shall be provided to the supervening defence counsel in original format, if this is the format in which they are kept.

4. Controllership in respect of the processing shall not be terminated merely because of the suspension and/or termination of one's professional activity. In case of termination also due to supervening impediments, and if no substitute defence counsel is available in respect of the given case, the documents related to past case files shall be delivered to the relevant Council – after expiry of a suitable period following communication to one's client – so that they can be kept for defence purposes.

Article 5 – Data Communication and Dissemination

1. As for relationships with the press and third parties, non-confidential information may be provided if this is necessary to safeguard one's client – regardless of whether this has been agreed upon with the said client – in compliance with the principles of purpose limitation, lawfulness, fairness, data minimization, relevance and non-excessiveness as per Section 11 of the DP Code as well as by respecting the data subject's and third parties' rights and dignity, any prohibitions set forth in the law, and the Code of practice of the Bar.

Article 6 – Inquiries Concerning Documents Held by Defence Counsel

1. Whenever a lawyer is subject to inquiries and inspections, he/she shall be entitled – under section 159(3) of the DP Code – to arrange for the Chair of the competent Bar Council and/or a member of the Council acting on the Chair's behalf to attend. If the Chair is attending and so requests, a copy of the relevant order shall be delivered to him/her.
2. As for the requests to access or obtain communication of traffic data related to incoming phone calls under section 8(2)f. and section 24(1)f. of the DP Code, a lawyer shall certify to the provider of publicly available electronic communications services that the failure to obtain the said data will be actually and tangibly prejudicial to the performance of defence investigations; in doing so, he need not mention the case file number allocated to the given criminal proceeding.

Chapter III – Processing by Other Self-Employed Professionals and Other Entities

Article 7 – Application of Provisions Concerning Lawyers

1. The provisions set forth in Articles 2 and 5 shall apply to the following entities without prejudice to what is applicable by law exclusively to lawyers:
    a. Self-employed professionals providing advisory and assistance services to establish or defend a judicial claim and/or to carry out defence investigations whether after being entrusted therewith by a lawyer and/or jointly with a lawyer and/or in the cases and to the extent permitted by the law;
    b. Any other entities mentioned in Article 1(2) subject to what is manifestly incompatible with the individual entity and/or the function discharged by the said entity.

Chapter IV – Processing by Private Detectives

Article 8 – Processing Mechanisms

1. A private detective shall arrange for the processing of personal data, whether automated or not, to be compliant with the requirements laid down in Article 2(1).
2. A private detective may not undertake investigations, surveys and any other type of data collection on their own initiative. The said activities may only be carried out if the detective has been hired on purpose via a written agreement and they may only be aimed at the purposes mentioned in this Code.

3. The hiring agreement must refer specifically to the right to be established before a judicial authority, or else the criminal proceeding the investigation relates to, along with the main factual elements accounting for the said investigation and the reasonable deadline for concluding the investigation.
4. A private detective shall discharge the task committed to him/her in person by only availing himself/herself of such additional detectives as are referred to individually in the hiring agreement; the names of the said additional detectives may be appended subsequently to the agreement if this option is envisaged therein. The provisions applying to the processing of sensitive data as set forth in the Garante's authorisations shall be left unprejudiced.
5. Where a private detective avails himself/herself of in-house staff as either data processors or persons in charge of the processing pursuant to sections 29 and 30 of the DP Code, he/she shall issue specific instructions on the arrangements to be abided by and supervise – at least on a weekly basis – that the applicable laws and instructions are complied with.
6. The defence counsel and/or the hiring entity must be informed regularly on the progress made with the investigations; this is also meant to allow them to timely assess what decisions to make in respect of establishing the judicial claim and/or exercising the right to evidence.

Article 9 – Other Rules of Conduct

1. A private detective shall refrain from any practices that fail to conform with legal obligations and constraints; in particular, a private detective shall ensure that the following are in line with the lawfulness and fairness standards laid down in the DP Code:
    a. Acquisition of personal data from other data controllers, including browsing of such data, whereby it shall be verified that one is entitled to obtain the data in question;
    b. Deployment of lawful monitoring activities, especially remote monitoring, and video/audio recording;
    c. Collection of biometric data.

2. A private detective shall comply with the provisions set forth in Article 2(4) to (6) of this Code when processing data.

Article 10 – Data Retention and Erasure

1. Under the terms of section 11(1)e. of the DP Code, any personal data that is processed by a private detective may be kept for no longer than is absolutely necessary to discharge the task committed. To that end, it shall be necessary to continuously verify that the data are closely relevant, not excessive and indispensable by having regard to the purposes sought and the task committed as above; regular controls may be carried out for this purpose.
2. Upon completion of the specific investigation, the processing must be discontinued in all respects except for the immediate communication of the data to the defence counsel and/or the hiring entity; the latter may allow – also via a specific assignment – that closely personal items related to the entities that have dealt with the relevant activities be retained, on a provisional basis, exclusively in order to provide proof that their conduct was lawful and fair. If the processing has been challenged, the defence counsel and/or the hiring entity may also provide the detective with such items as are required to provide proof that their conduct was lawful and fair – for no longer than this is absolutely necessary.
3. The fact that the proceeding underlying the given investigation is as yet pending, or that the case was brought before a higher-instance court pending the final judgment, does not represent in itself a valid justification for the private detective to retain the data.

Article 11 – Information Notice

1. A private detective may provide the information notice at a single juncture in pursuance of Article 3 hereof by highlighting the detective's identity and professional capacity as well as the circumstance that the data are provided on an optional basis.

Chapter V – Final Provisions

Article 12 – Monitoring Implementation of the Code

1. Under section 135 of the DP Code, the signatories to this code shall undertake collaboration initiatives to regularly monitor its implementation also with a view to making such adjustments as may be appropriate in the light of technological developments, experience and/or regulatory changes.

Article 13 – Entry into Force

1. This code shall apply as from 1 January 2009.

TECHNICAL SPECIFICATIONS CONCERNING MINIMUM SECURITY MEASURES (ANNEX B)

(see Sections 33 to 36 of the Code)

PROCESSING BY ELECTRONIC MEANS

The following technical arrangements to be implemented by the data controller, data processor – if nominated – and person(s) in charge of the processing whenever data are processed by electronic means:

Computerised Authentication System

1. Persons in charge of the processing shall be allowed to process personal data by electronic means if they are provided with authentication credentials such as to successfully complete an authentication procedure relating either to a specific processing operation or to a set of processing operations.

2. Authentication credentials shall consist in an ID code for the person in charge of the processing as associated with a secret password that shall only be known to the latter person; alternatively, they shall consist in an authentication device that shall be used and held exclusively by the person in charge of the processing and may be associated with either an ID code or a password, or else in a biometric feature that relates to the person in charge of the processing and may be associated with either an ID code or a password.

3. One or more authentication credentials shall be assigned to or associated with each person in charge of the processing.

4. The instructions provided to the persons in charge of the processing shall lay down the obligation to take such precautions as may be necessary to ensure that the confidential component(s) in the credentials are kept secret and that the devices used and held exclusively by persons in charge of the processing are kept with due care.

5. Where provided for by the relevant authentication system, a password shall consist of at least eight characters; if this is not allowed by the electronic equipment, a password shall consist of the maximum permitted number of characters. It shall not contain any item that can be easily related to the person in charge of the processing and shall be modified by the latter when it is first used as well as at least every six months thereafter. If sensitive or judicial data are processed, the password shall be modified at least every three months.

6. An ID code, if used, may not be assigned to another person in charge of the processing even at a different time.

7. Authentication credentials shall be de-activated if they have not been used for at least six months, except for those that have been authorised exclusively for technical management purposes.

8. Authentication credentials shall be also de-activated if the person in charge of the processing is disqualified from accessing personal data.

9. The persons in charge of the processing shall be instructed to the effect that electronic equipment should not be left unattended and made accessible during processing sessions.

10. Where data and electronic equipment may only be accessed by using the confidential component(s) of the authentication credential, appropriate instructions shall be given in advance, in writing, to clearly specify the mechanisms by which the data controller can ensure that data or electronic equipment are available in case the person in charge of the processing is either absent or unavailable for a long time and it is indispensable to carry out certain activities without further delay exclusively for purposes related to system operationality and security. In this case, copies of the credentials shall be kept in such a way as to ensure their confidentiality by specifying, in writing, the entities in charge of keeping such credentials. Said entities shall have to inform the person in charge of the processing, without delay, as to the activities carried out.

11. The provisions concerning the authentication system referred to above as well as those concerning the authorisation system shall not apply to the processing of personal data that are intended for dissemination.

Authorisation System

12. Where authorisation profiles with different scope have been set out for the persons in charge of the processing, an authorisation system shall be used.

13. Authorisation profiles for each person or homogeneous set of persons in charge of the processing shall be set out and configured prior to start of the processing in such a way as to only enable access to the data that are necessary to perform processing operations.

14. It shall be regularly verified, at least at yearly intervals, that the prerequisites for retaining the relevant authorisation profiles still apply.

Other Security Measures

15. Within the framework of the regular update – to be performed at least at yearly intervals – of the specifications concerning the scope of the processing operations that are entrusted to the individual persons in charge of the processing as well as to the technicians responsible for management and/or maintenance of electronic equipment, the list of the persons in charge of the processing may also be drawn up by homogeneous categories of task and corresponding authorisation profile.

16. Personal data shall be protected against the risk of intrusion and the effects of programmes as per Section 615-quinquies of the Criminal Code by implementing suitable electronic means to be updated at least every six months.

17. The regular update of computer programmes as aimed at preventing vulnerability and removing flaws of electronic means shall be carried out at least annually. If sensitive or judicial data are processed, such update shall be carried out at least every six months.

18. Organisational and technical instructions shall be issued such as to require at least weekly data back-ups.

Security Policy Document

19. By 31 March of each year, the controller of processing operations concerning sensitive and/or judicial data shall draw up, also by the agency of the data processor, if nominated, a security policy document containing appropriate information with regard to:

19.1 the list of processing operations concerning personal data,
19.2 the distribution of tasks and responsibilities among the departments/divisions in charge of processing data,
19.3 an analysis of the risks applying to the data,
19.4 the measures to be taken in order to ensure data integrity and availability as well as protection of areas and premises insofar as they are relevant for the purpose of keeping and accessing such data,
19.5 a description of the criteria and mechanisms to restore data availability following destruction and/or damage as per point 23 below,
19.6 a schedule of training activities concerning the persons in charge of the processing with a view to informing them on the risks applying to the data, the measures that are available to prevent harmful events, the most important features of personal data protection legislation in connection with the relevant activities, the resulting liability and the arrangements to get updated information on the minimum security measures adopted by the data controller. Said training activities shall be planned as of the start of the employment relationship as well as in connection with changes in the task(s) discharged and/or the implementation of new, significant means that are relevant to the processing of personal data,
19.7 a description of the criteria to be implemented in order to ensure adoption of the minimum security measures whenever processing operations concerning personal data are externalised in accordance with the Code,
19.8 as for the personal data disclosing health and sex life referred to under point 24, the specification of the criteria to be implemented in order to either encrypt such data or keep them separate from other personal data concerning the same data subject.

Additional Measures Applying to Processing of Sensitive or Judicial Data

20. Sensitive or judicial data shall be protected against unauthorised access as per Section 615-ter of the Criminal Code by implementing suitable electronic means.

21. Organisational and technical instructions shall be issued with regard to keeping and using the removable media on which the data are stored in order to prevent unauthorised access and processing.

22. The removable media containing sensitive or judicial data shall be destroyed or made unusable if they are not used; alternatively, they may be re-used by other persons in charge of the processing, who are not authorised to process the same data, if the information previously contained in them is not intelligible and cannot be re-constructed by any technical means.

23. If either the data or electronic means have been damaged, suitable measures shall be adopted to ensure that data access is restored within a specific deadline, which must be compatible with data subjects' rights and not in excess of seven days.

24. Health care bodies and professionals shall process data disclosing health and sex life as contained in lists, registers or data banks in accordance with the mechanisms referred to in Section 22(6) of the Code also in order to ensure that said data are processed separately from the other personal data allowing data subjects to be identified directly. Data concerning genetic identity shall only be processed in protected premises that may only be accessed by such persons in charge of the processing and entities as have been specifically authorised to access them. Containers equipped with locks or equivalent devices shall have to be used in order to remove the data outside the premises reserved for their processing; the data shall have to be encrypted for the purpose of electronically transferring them.

Safeguards and Protections

25. Where a data controller adopts minimum security measures by committing the relevant tasks to external entities, prior to implementing such measures he or she shall require the installing technician(s) to supply a written description of the activities performed by which it is certified that they are compliant with the provisions set out in these technical specifications.

26. The circumstance that the security policy document has been drawn up and/or updated shall be referred to in the management report that the data controller may be required to submit together with the relevant balance sheet.

PROCESSING WITHOUT ELECTRONIC MEANS

The following technical arrangements to be implemented by the data controller, data processor – if nominated – and person(s) in charge of the processing whenever data are processed without electronic means:

27. The persons in charge of the processing shall be instructed in writing with regard to controlling and keeping, throughout the steps required to perform processing operations, records and documents containing personal data. Within the framework of the regular update – to be performed at least at yearly intervals – of the specifications concerning the scope of the processing operations that are entrusted to the individual persons in charge of the processing, the list of the persons in charge of the processing may also be drawn up by homogeneous categories of task and corresponding authorisation profile.

28. If records and documents containing sensitive or judicial personal data are entrusted to the persons in charge of the processing for the latter to discharge the relevant tasks, said records and documents shall be kept and controlled by the persons in charge of the processing until they are returned so as to prevent unauthorised entities from accessing them; they shall be returned once the relevant tasks have been discharged.

29. Access to archives containing sensitive or judicial data shall be controlled. The persons authorised to access said archives for whatever purpose after closing time shall be identified and registered. If an archive is not equipped with electronic devices for access control or is not placed under the surveillance of security staff, the persons accessing said archive shall have to be authorised in advance.