PERSONAL DATA PROTECTION CODE
Containing provisions to adapt the national legislation to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Text released on 26.03.2020
(as amended by Law No 160 of 27 December 2019)

TABLE OF CONTENTS

THE PRESIDENT OF THE REPUBLIC

HAVING REGARD to Articles 76 and 87 in the Constitution,

HAVING REGARD to Section 1 of Law 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 Law No 14 of 3 February 2003, setting out provisions to ensure compliance with obligations related to Italy's membership in the European Communities (Community Law of 2002),

HAVING REGARD to Law No 675 of 31 December 1996 as subsequently amended,

HAVING REGARD to Law 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:[1]

[1] The word "subscriber" was replaced by "contracting party" throughout legislative decree No 196/2003 pursuant to Section 1(12) of legislative decree No 69 dated 28 May 2012.

PART 1 – PRINCIPLES

TITLE I – PRINCIPLES AND GENERAL PROVISIONS

CHAPTER I – SCOPE, PURPOSES AND SUPERVISORY AUTHORITY

Section 1

(Scope)

1. Personal data shall be processed in accordance with the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, hereinafter the 'Regulation', and with this Code, by respecting human dignity and the rights and fundamental freedoms of the individual.

Section 2

(Purposes)

1. This Code lays down the provisions to adapt the national legislation to the provisions of the Regulation.

Section 2-a

(Supervisory dAuthority)

1.The supervisory authority referred to in Article 51 of the Regulation shall be the Garante per la protezione dei dati personali, hereinafter the 'Garante', as per Section 153 hereof.

CHAPTER II – PRINCIPLES

Section 2-b

(*Legal basis to process personal data for the performance of a task carried out in the public interest or in the exercise of official authority)*

1. The legal basis mentioned in Article 6(3), letter b), of the Regulation shall only be either a law or, where so provided for by a law, a regulation.
2. Personal data other than those belonging to the special categories referred to in Article 9 of the Regulation or relating to criminal convictions and offences referred to in Article 10 of

the Regulation may be communicated between controllers processing such personal data for the performance of a task carried out in the public interest or in the exercise of official authority if this is provided for in accordance with paragraph 1 hereof. Failing this, communication shall be permitted if it is necessary to carry out tasks in the public interest or to fulfil institutional duties and may commence upon expiry of a 45-day period after informing the Garante thereof if the latter has not decided otherwise regarding the measures to be taken in order to safeguard data subjects.

3. Personal data that are processed for the performance of a task carried out in the public interest or in the exercise of official authority may be disseminated or communicated to entities that are intending to process such data for other purposes exclusively if this is provided for in accordance with paragraph 1 hereof.
4. *a)* 'Communication' shall mean disclosing personal data in whatever manner, including by making available, interrogating or creating links to such data, to one or more identified entities other than the data subject, the controller's representative in the EU, the processor or the latter's representative in the EU, and the persons authorised to process personal data under the controller's or processor's authority in pursuance of Section 2-m;
   (b) 'Dissemination' shall mean disclosing personal data in whatever manner, including by making available or interrogating such data, to unidentified entities.

Section 2-c

(Rules of Conduct)

1. Giving consideration to the representativeness principle and taking account of the recommendations by the Council of Europe on the processing of personal data, the Garante shall promote the adoption of rules of conduct for the processing activities referred to in Article 6(1), letters c) and e), Article 9 and Chapter IX of the Regulation, verify that such rules are in compliance with the provisions in force by also evaluating the observations submitted by relevant stakeholders, and contribute to ensuring that such rules are disseminated and abided by.
2. A public consultation of at least 60-day duration shall be launched on the draft rules of conduct.
3. Upon closure of the consultation phase, the rules of conduct shall be approved by the Garante pursuant to Section 154-a, paragraph 1, letter b), published in the Official Journal of the Italian Republic, and included in Annex A to this Code by a decree of the Minister of Justice.
4. Compliance with the provisions set out in the rules of conduct referred to in paragraph 1 shall be a fundamental precondition for the processing of personal data to be lawful and fair.

Section 2-d

(Child's Consent in Relation to Information Society Services)

1. Pursuant to Article 8(1) of the Regulation, a child aged above 14 years may give his or her consent to the processing of his or her personal data in relation to the offer of information society services directly to him or her. Regarding such services, the personal data of a child aged below 14 years may be processed lawfully in accordance with Article 6(1), letter a) of the Regulation if the consent is given by the holder of parental responsibility over the child.

2. In relation to the offer of the services referred to in paragraph 1 directly to a child, the controller shall provide any information and communication relating to the processing activities concerning that child by using clear and plain language, in an especially concise, exhaustive, easily accessible and intelligible form, so as to make the child's consent meaningful.

Section 2-e

(Processing of Special Categories of Personal Data That Is Necessary for Reasons of Substantial Public Interest)

1. Processing of the special categories of data referred to in Article 9(1) of the Regulation that is necessary for reasons of substantial public interest in accordance with paragraph 2, letter g) thereof shall be allowed if it is provided for in EU law or, as regards the national legal system, in a law or, where so provided for by a law, a regulation; such law or regulation shall specify what types of data may be processed, what processing activities may be performed and what substantial public interest reasons justify the processing along with the suitable, specific measures to safeguard the data subject's fundamental rights and interests.
2. Without prejudice to paragraph 1, a substantial public interest shall be considered to exist in relation to processing activities performed by entities that carry out tasks in the public interest or in the exercise of official authority in the following sectors:
    a. Access to administrative records and FOIA procedures;
    b. Keeping the registries and certificates of births, deaths and marriages, the census register of residents in Italy and Italian nationals residing abroad, and electoral registers, and issuance of identity, travel or change of identification data documents and records;
    c. Keeping public registries of movable or immovable property;
    d. Keeping the national register of the holders of driving licenses and the national register of vehicles;
    e. Citizenship, immigration, asylum, aliens or displaced persons, refugee status;
    f. Right to vote and be elected and exercise of other political rights, diplomatic or consular safeguards, documenting the institutional activities of public bodies with particular regard to the drawing up of minutes and reports of the activities of representatives' assemblies, committees and any other collegiate body or assembly;
    g. Exercising the mandate conferred on representation bodies including suspension or dissolution of such bodies and establishing grounds for ineligibility as a candidate, incompatibility with or disqualification, dismissal or suspension from public offices;
    h. Carrying out oversight, political guidance, parliamentary inquiry or parliamentary review tasks and enabling access to documents and records as provided for by law and the rules of procedure of the relevant bodies exclusively for purposes that are directly related to the discharge of the electoral mandate;
    i. Activities by public bodies intended to implement taxation and customs-related provisions, also by the agency of the respective licensees, including preventing and countering tax evasion[2];
    l. Supervisory and inspection activities;
    m. Granting, payment, modification and revocation of allowances, benefits, donations, other amounts and permissions;

[2] Amended by Section 1(681) of Law No 160 of 27 December 2019.

n. Awarding of honours and compensations; recognition of the legal personality of associations, foundations and organizations, including religious confessions; establishing, when this falls under the scope of a public body's competence, the eligibility and professional qualifications for the appointment to official positions, also related to religious confessions, as well as for the appointment to senior positions in legal persons, companies and non-public educational bodies; and issuance and revocation of authorisations or permissions, granting of sponsorships, patronage and medals or Presidential seals, joining committees of honour and admission to institutional ceremonies and meetings;
o. Relationships between public bodies and no-profit organisations;
p. Conscientious objection;
q. Imposition of administrative or judicial sanctions and safeguards;
r. Institutional relationships with religious bodies, confessions or communities;
s. Welfare-related activities to protect children and frail, non-self-sufficient or incapacitated individuals;
t. Administrative activities and issuance of certifications in connection with health care and welfare activities (diagnosis, assistance, treatment) including organ and tissue transplantations and human blood transfusions;
u. Tasks committed to the national health service and health care practitioners; tasks related to occupational safety, population health and safety, civil protection, protection of life and bodily integrity;
v. Planning, management, monitoring and assessment of health care including establishment, management, planning and monitoring of relationships between health care bodies and the entities accredited with or outsourced to by such bodies;
z. Oversight over experimental activities, pharmacovigilance, granting authorisations with a view to marketing and importing drugs and other health-relevant products;
aa. Protection of motherhood, termination of pregnancy, handling of addictions, assistance to, social integration and rights of the disabled;
bb. Providing education and training at school, vocational, university or post-university level;
cc. Processing activities performed for archiving purposes in the public interest or for historical research purposes concerning preservation, cataloguing and communication of documents and records held in State archives, historical archives of public bodies, or private archives declared to be of especially substantial historical interest; processing activities for purposes of scientific research and processing for statistical purposes by entities belonging to the national statistics system (Sistan);
dd. Establishing, managing and terminating labour relations of any kind whatsoever, including unpaid, honorary, and other types of employment, trade union-related matters, implementing the provisions concerning mandatory employment of disabled persons, handling welfare and social security policies, protecting minorities and ensuring equal opportunity policies in employer-employee relations, fulfilling obligations concerning wages, taxation or accounting in respect of staff, or concerning occupational hygiene and safety, population health and safety, and carrying out activities aimed at establishing civil, disciplinary and accounting liability and performing inspection activities.

3. As for genetic data, biometric data and data relating to health, processing shall be carried out in all cases pursuant to Section 2-f hereof.

Section 2-f

(Safeguards applying to the processing of genetic data, biometric data, and data relating to health)

1. Pursuant to Article 9(4) of the Regulation, genetic data, biometric data and data relating to health may be processed if one of the conditions mentioned in paragraph 2 of the said article is fulfilled and in compliance with the safeguards set out by the Garante in accordance with this Section.
2. The provision setting out the safeguards referred to in paragraph 1 shall be adopted at least every other year by taking account of the following:
    a. The guidelines, recommendations and best practices published by the European data protection board and the best practices concerning the processing of personal data;
    b. The scientific and technological developments in the sector addressed by the safeguards;
    c. The interest in the free movement of personal data in the EU.
3. The draft of the aforementioned provision shall be subjected to a public consultation for a period of at least sixty days.
4. The safeguards shall be adopted in compliance with Article 9(2) of the Regulation and also concern the precautions to be taken with regard to the following:
    a. Vehicle permit stickers and accesses to restricted access areas;
    b. Organisational and management issues in health care;
    c. Arrangements to directly inform data subjects of diagnoses and data relating to their health;
    d. Drug prescriptions.
5. The safeguards shall be adopted in respect of each category of personal data as per paragraph 1 by having regard to the specific purposes of the processing and may lay down, pursuant to paragraph 2, additional conditions to be fulfilled for the processing of the said data to be allowed. In particular, the safeguards in question shall set out the security measures including encryption and pseudonymisation techniques, minimisation measures, the specific arrangements to enable selective access to the data and provide information to data subjects, and such additional measures as may be necessary to safeguard data subjects' rights.
6. The safeguards concerning genetic data and the processing of data relating to health for prevention, diagnosis and treatment purposes as well as the safeguards referred to in paragraph 4, letters b) ad c) above shall be adopted after hearing the Ministry of Health, which shall obtain, for that purpose, an opinion from the Consiglio Superiore di Sanità (Higher Council for Health Care). As regards genetic data, the safeguards may provide for relying on the data subject's consent as an additional measure to protect the data subject's rights in case a particular high risk exists, pursuant to Article 9(4) of the Regulation, or set out any additional specific precautions.
7. Biometric data may be used with regard to the procedures enabling physical or logical access to data by authorised entities, by having regard to the obligations mentioned in Article 32 of the Regulation, in accordance with personal data protection principles and providing the safeguards referred to in this Section are complied with.
8. The personal data mentioned in paragraph 1 may not be disseminated.

Section 2-g

(Principles applying to the processing of data relating to criminal convictions and offences)

1. Subject to the provisions made in legislative decree No 51 of 18 May 2018, processing of personal data relating to criminal convictions and offences or related security measures as based on Article 6(1) of the Regulation that is not carried out under the control of official authority shall be allowed solely if it is authorised by a law or, where so provided for by law, by a regulation providing for appropriate safeguards for the rights and freedoms of data subjects, in accordance with Article 10 of the Regulation.
2. Failing the aforementioned provisions in laws or regulations, the data processing activities referred to in paragraph 1 and the safeguards mentioned therein shall be specified by a decree of the Minister of Justice to be adopted after hearing the Garante pursuant to Section 17(3) of Law No 400 of 23 August 1988.
3. Without prejudice to paragraphs 1 and 2 above, processing of data relating to criminal convictions and offences or related security measures shall be allowed if authorised by a law or, where so provided for by law, by a regulation concerning, in particular,
    a. Fulfilment of obligations and exercise of rights by the controller or data subject in connection with labour law or within the framework of employer-employee relations under the terms set out in laws, regulations and collective agreements and in pursuance of Article 9(2), letter b), and Article 88 of the Regulation;
    b. Fulfilment of the obligations set out in laws or regulations concerning mediation for the purpose of resolving civil and commercial disputes;
    c. Verification or establishment of the absence of criminal records, personal qualifications and disqualifications where so provided for by laws or regulations;
    d. Determination of liability for accidents or events relating to human life, and preventing, detecting or countering fraud or situations of factual risk to the appropriate performance of insurance activities under the terms set out in the relevant laws or regulations;
    e. Establishing, exercising or defending a legal claim;
    f. Exercising the right to access data and documents held by administrative bodies under the terms set out in the relevant laws or regulations;
    g. Carrying out investigations or researches or collecting information on behalf of third parties under the terms of Section 134 of the consolidated statute on public security;
    h. Fulfilment of obligations arising from laws regulating communications and notifications required to counter Mafia-type crime or aimed at preventing the commission of Mafia-type offences and other serious types of socially dangerous crime where so provided for by laws or regulations, or else with a view to submitting the documents required by law to participate in tenders;
    i. Establishing the moral qualifications required for participating in tenders pursuant to the applicable legislation;
    l. Implementation of the legislation concerning the legality rating of businesses pursuant to Section 5-b of Decree-law No 1 of 24 January 2012 as enacted, including amendments thereof, by Law No 27 of 24 March 2012;
    m. Fulfilment of the obligations set out in the applicable legislation concerning prevention of the use of the financial system for the purpose of laundering the proceeds of crime and financing terrorism.
4. Where the instruments referred to in paragraph 3 do not specify the appropriate safeguards for the rights and freedoms of data subjects, the safeguards in question shall be laid down in the decree mentioned in paragraph 2.

5. Where processing of the data mentioned in this Section is carried out under the control of official authority, the provisions of Section 2-e shall apply.
6. Processing of the data referred to in Article 10 of the Regulation as carried out in pursuance of memorandums of understanding to prevent and counter organised crime that are entered into with the Ministry of the Interior and/or local governmental offices ('prefetture') shall be authorised via the decree mentioned in paragraph 2. As regards such memorandums, the decree referred to in paragraph 2 shall specify the types of data processed, the data subjects, and the processing activities permitted as also related to updating and storage of the data; it shall also lay down the appropriate safeguards for the rights and freedoms of data subjects. The decree shall be adopted in agreement with the Ministry of the Interior with regard to the subject matters referred to in this paragraph.

Section 2-h

(Processing activities regulated by the Presidency of the Republic, the Chamber of Deputies, the Senate of the Republic, the Constitutional Court)

1. The provisions contained in sections 2-e, 2-f and 2-g of this legislative decree lay down principles that are applicable, in accordance with the respective regulatory systems, to the processing of the personal data categories as per Articles 9(1) and 10 of the Regulation that is regulated by the Presidency of the Republic, the Chamber of Deputies, the Senate of the Republic and the Constitutional Court.

Section 2-i

(Non-usability of data)

1. Personal data that is processed in breach of the relevant provisions on the processing of personal data may not be used except as provided for in Section 160-a.

CHAPTER III - PROVISIONS ON THE RIGHTS OF DATA SUBJECTS

Section 2-l

(Restrictions on the rights of data subjects)

1. The rights referred to in Articles 15 to 22 of the Regulation may not be exercised by making a request to the controller or lodging a complaint pursuant to Article 77 of the Regulation if the exercise of those rights may prove factually, effectively detrimental to any of the following:
    a. The interests safeguarded by anti-money laundering provisions;
    b. The interests safeguarded by the provisions aimed to support victims of extortion;
    c. The activities of parliamentary enquiry committees as set up pursuant to Article 82 of the Constitution;
    d. The activities carried out by a public body other than a profit-seeking organisation as expressly provided for by a law for purposes relating exclusively to monetary

policies, the system of payments, the oversight over credit and financial brokers and markets, and the protection of market stability;

e. The performance of investigations by defence counsel or the exercise of a legal claim;

f. Confidentiality regarding the identity of whistleblowers pursuant to Law No 179 of 30 November 2017;

f-a. Protected interests regarding taxation and the performance of activities aimed at preventing and countering tax evasion. [3]

2. In the cases referred to in paragraph 1, letter c), the provisions contained in parliamentary rules of procedures, laws or the instruments setting up the individual enquiry committee shall apply.
3. In the cases referred to in paragraph 1, letters a), b), d), e), f), and f-a), the rights as per the said paragraph shall be exercised in accordance with the laws or regulations applying to the individual sectors, which must contain at least measures aimed at regulating the matters mentioned in Article 23(2) of the Regulation. Exercise of the rights in question may be delayed, restricted or ruled out, in which case the data subject shall be informed of the relevant reasons without delay except where that may be prejudicial to the purpose of the restriction, for as long as and to the extent this is a necessary and proportionate measure by taking account of the fundamental rights and legitimate interests of the data subject in order to protect the interests mentioned in paragraph 1, letters a), b), d), e), f) and f-a). In that case, the rights of the data subject may be exercised also through the Garante in accordance with the arrangements set out in Section 160. Where this is so, the Garante shall inform the data subject that all the necessary verifications have been carried out or that a review has been carried out, and that the data subject has the right to complain before a judicial authority. The controller shall inform the data subject of the arrangements available as per this paragraph.[4]

Section 2-m

(Restrictions based on judicial grounds)

1. Further to Article 23(1), letter f), of the Regulation, the rights and obligations referred to in Articles 12 to 22 and 34 of the Regulation as related to the processing of personal data that is carried out on judicial grounds in connection with proceedings before judicial offices of all types and levels as well as before the Consiglio Superiore della Magistratura (Higher Judicial Council) and any other self-governance bodies of special judicial authorities or before the Ministry of Justice shall be regulated under the terms of and in accordance with the arrangements set out in the laws or regulations applicable to the said proceedings as well as in compliance with Article 23(2) of the Regulation.
2. Without prejudice to paragraph 1, exercise of the rights and fulfilment of the obligations referred to in Articles 12 to 22 and 34 of the Regulation may be delayed, restricted or ruled out, in which case the data subject shall be informed of the relevant reasons without delay except where that may be prejudicial to the purpose of the restriction, to the extent and for as long as this is a necessary and proportionate measure by taking account of the fundamental rights and legitimate interests of the data subject in order to protect independency of the judiciary and judicial proceedings.
3. Section 2-l, paragraph 3, third, fourth and fifth sentence shall apply.
4. For the purposes of this Section, processing activities on judicial grounds shall mean any processing of personal data that is related to the handling of cases and disputes at judicial

[3] Amended by Section 1(681) of Law No 160 of 27 December 2019.
[4] Amended by Section 1(681) of Law No 160 of 27 December 2019.

level, the processing activities carried out with regard to the legal status and payment conditions applicable to the judiciary, and the processing activities that are carried out in connection with inspections concerning judicial offices. Judicial grounds do not include the standard management and administrative activities concerning staff, equipment or facilities providing this is not prejudicial to the confidentiality of instruments that are related directly to the handling of proceedings at judicial level.

Section 2-n

(Rights concerning deceased persons)

1. The rights referred to in Articles 15 to 22 of the Regulation concerning the personal data of deceased persons may be exercised by any entity having a vested interest or acting to protect the data subject as the latter's agent, or else on household-related grounds deserving protection.
2. Exercise of the rights referred to in paragraph 1 shall not be allowed where so provided for in a law or if the data subject has banned such exercise expressly by means of a written statement submitted or communicated to the controller with regard to the direct offer of information society services.
3. The data subject's intention to ban exercise of the rights referred to in paragraph 1 must be unambiguous, specific, free and informed. The ban may apply to the exercise of some of the rights referred to in the said paragraph.
4. The data subject has the right to at any time revoke or amend the ban referred to in paragraphs 2 and 3.
5. The ban shall in no case result into detrimental effects to the exercise by third parties of property rights arising from the data subject's decease or of the right to defend a legal claim.

CHAPTER IV – PROVISIONS ON CONTROLLERS AND PROCESSORS

Section 2-o

(Allocation of tasks and functions to designated entities)

1. The controller or processor may provide under their own responsibility and within the framework of the respective organisation that specific tasks and functions relating to the processing of personal data be allocated to expressly designated natural persons acting under the controller's or processor's authority.
2. The controller or processor shall set out the most appropriate arrangements to authorise the persons acting under their authority to process personal data.

Section 2-p

(Processing entailing a high risk for the performance of a task carried out in the public interest)

1. With regard to processing that is carried out for the performance of a task in the public interest and may entail a high risk under Article 35 of the Regulation, the Garante may lay down measures and arrangements to protect data subjects, which the controller shall be required to implement, in accordance with Article 36(5) thereof and by way of decisions of general application adopted of its own motion.

Section 2-q

(Appointment of a data protection officer in connection with processing carried out by judicial authorities acting in their capacity as such)

1. A data protection officer shall also be appointed with regard to the processing of personal data that is carried out by judicial authorities acting in their capacity as such, pursuant to the provisions contained in Section 4 of Chapter IV of the Regulation.

Section 2-r

(National accreditation body)

1. The national accreditation body referred to in Article 43(1), letter b), of the Regulation shall be the single national accreditation body as set up in accordance with Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008, subject to the Garante's power to directly take up the exercise of the relevant functions following a resolution to be published in the Official Journal of the Italian Republic, also with regard to one or more than one type of processing, in case the single national accreditation body is seriously in breach of its duties.

Section 3

(Data Minimisation Principle)

(repealed)

Section 4

(Definitions)

(repealed)

Section 5

(Subject-Matter and Scope of Application)

(repealed)

Section 6

(Regulations Applying to Processing Operations)

(repealed)

TITLE II – DATA SUBJECT'S RIGHTS

(repealed)

TITLE III – GENERAL DATA PROCESSING RULES

(repealed)

TITLE IV – ENTITIES PERFORMING PROCESSING OPERATIONS

(repealed)

TITLE V – DATA AND SYSTEM SECURITY

(repealed)

TITLE VI – PERFORMANCE OF SPECIFIC TASKS

(repealed)

TITLE VII – TRANSBORDER DATA FLOWS

(repealed)

PART II – PROVISIONS APPLYING TO PROCESSING THAT IS NECESSARY FOR COMPLIANCE WITH A LEGAL OBLIGATION OR FOR THE PERFORMANCE OF A TASK CARRIED OUT IN THE PUBLIC INTEREST OR IN THE EXERCISE OF OFFICIAL AUTHORITY AND PROCESSING REFERRED TO IN CHAPTER IX OF THE REGULATION

TITLE 0.I – PROVISIONS ON THE LEGAL BASIS

Section 45-a

(Legal basis)

1. The provisions contained in this part are laid down in pursuance of Article 6(2) and Article 23(1) of the Regulation.

TITLE I – PROCESSING OPERATIONS IN THE JUDICIAL SECTOR

CHAPTER I – IN GENERAL

(repealed)

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. Violation of the prohibition referred to herein shall be punished in pursuance of Section 684 of the Criminal Code.

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.

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 209 of the Consolidated Statute on public procurement referred to in legislative decree No 50 of 18 April 2016 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[5]

CHAPTER I – IN GENERAL

Section 53

(repealed)

Section 54

(repealed)

Section 55

(repealed)

Section 56

(repealed)

Section 57[6]

(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

[5] Sections 53 to 56 were repealed by Section 49(1) of legislative decree No 51 of 18 May 2018 implementing EU Directive 2016/680 of the European Parliament and of the Council, of 27 April 2016, on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

[6] Section 49(2) of the aforementioned legislative decree provided that Section 57 would be repealed after one year from entry into force of the decree.

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 all of the following:

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

(Processing of personal data for purposes of national security or defence)

1. Processing of personal data that is carried out by the entities referred to in Sections 4, 6 and 7 of Law No 124 of 3 August 2007 in pursuance of Section 26 of the said Law or else of other laws or regulations, and processing that concerns data placed under State secrecy rules pursuant to Section 39 and ff. of the said law shall be regulated in accordance with Section 160(4) hereof as well as with Sections 2, 3, 8, 15, 16, 18, 25, 37, 41, 42, and 43 of legislative decree No 51 of 18 May 2018 where compatible.

2. Without prejudice to paragraph 1, processing that is carried out by public bodies for purposes of defence or State security in pursuance of statutory provisions that envisage such processing specifically shall be regulated by paragraph 1 hereof as well as by Sections 23 and 24 of legislative decree No 51 of 18 May 2018.

3. The implementing arrangements relating to the provisions referred to in paragraphs 1 and 2 shall be laid down in one or more than one regulations with regard to the types of data, data subjects, processing activities and persons authorised to process the personal data under the authority of the controller or processor pursuant to Section 2-o, including the relevant updating and storage mechanisms. The regulations applying to the subject matters under paragraph 1 shall be adopted in accordance with Section 43 of Law No 124 of 3 August 2007, and the regulations applying to the subject matters under paragraph 2 shall be adopted by way of a decree of the Prime Minister in accordance with Section 17(3) of Law No 400 of 23 August 1988, upon a proposal submitted by the competent Ministers.
4. The measures implementing this decree as related to the discharge of defence and national security functions by the armed forces shall be set out in one or more than one regulations adopted by a decree of the President of the Republic upon a proposal submitted by the Minister of defence.

TITLE IV – PROCESSING OPERATIONS IN THE PUBLIC SECTOR

CHAPTER I – ACCESS TO ADMINISTRATIVE RECORDS

Section 59

(Access to Administrative Records and FOIA-type access)

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 Law 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 data referred to in Articles 9 and 10 of the Regulation and the processing operations that may be performed to comply with a request for access.

1-a. The preconditions, arrangements and restrictions applying to exercise of FOIA-type access shall be regulated further by legislative decree No 33 of 14 March 2013.

Section 60

(Data relating to health, sex life or sexual orientation)

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 and Rules of Conduct)

1. The Garante shall encourage adoption, pursuant to Section 2-c, of rules of conduct 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 combining data from different archives, and by taking account of the relevant Council of Europe's Recommendations.

2. For the purposes of implementing this Code, personal data other than the data referred to in Articles 9 and 10 of the Regulation that are to be entered into a professional register pursuant to laws or regulations may be communicated to public and private bodies and disseminated pursuant to Section 2-b of this Code also by means of electronic communication networks. Reference may also be made to the existence of measures affecting the relevant professional practice on whatever grounds.

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

4. If the data subject so requests, 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

(Repealed)

CHAPTER IV – PURPOSES IN THE SUBSTANTIAL PUBLIC INTEREST

(Repealed)

CHAPTER V – SPECIFIC PERMITS

(Repealed)

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

CHAPTER I – IN GENERAL

Section 75

(Specific conditions applying to the health care sector)

1. Processing of personal data for the purpose of protecting the health and bodily integrity of the data subject, third parties or a community shall be carried out in accordance with Article 9(2), letters h) and i), and 9(3) of the Regulation and Article 2-f of this Code and by respecting the specific sector-related provisions.

Section 76

(Repealed)

CHAPTER II – SPECIFIC ARRANGEMENTS TO INFORM THE DATA SUBJECT AND PROCESS PERSONAL DATA

Section 77

(Specific arrangements)

1. This Title lays down specific arrangements that may be made by the entities referred to in paragraph 2 for any of the following purposes:

a) to inform the data subject in pursuance of Articles 13 and 14 of the Regulation;
b) to process personal data.

2. The arrangements referred to in paragraph 1 shall be applicable by any of the following:

a) public and private health care organisations providing health care and welfare services and health care professionals;
b) the 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 Articles 13 and 14 of the Regulation to be easily understandable.

2. The information may be provided as regards the overall personal data processing operations that are required for diagnosis, assistance and treatment activities 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 shall be given preferably in writing.

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; or

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 research purposes including clinical drug testing, in compliance with laws and regulations, by especially highlighting that the consent, where required, 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;

c-a) with a view to implementing the electronic health record referred to in Section 12 of decree-law No 179 of 18 October 2012 as enacted, including amendments thereof, by Law No 221 of 17 December 2012; or

c-b) for the purposes of the monitoring systems and registries referred to in Section 12 of decree-law No 179 of 18 October 2012 as enacted, including amendments thereof, by Law No 221 of 17 December 2012.

Section 79

(Information by public and private organisations providing health care and welfare services)

1. Public and private organisations providing health care and welfare services may avail themselves of the specific arrangements referred to in Section 78 with regard to a number of services provided also by different divisions and units within those organisations or in specified hospitals or local branches of such organisations.

2. In the cases referred to in paragraph 1, the organisation or its branches shall record the information provided in a unified manner so 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 specific arrangements referred to in Section 78 may be implemented 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 specific 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 Entities)

1. In addition to the provisions made in Section 79, the competent services or departments of public bodies other than those mentioned in the said Section 79 that deal with health care or social protection and welfare matters may avail themselves, in providing the information referred to in Articles 13 and 14 of the Regulation, of the possibility to provide a single information notice in connection with a number of processing operations performed for administrative purposes and at different times with regard to data collected from the data subject or from third parties.

2. The information as per paragraph 1 shall be supplemented by means of suitable, specific notices and signs, which shall be easily visible to the public, to be posted and disseminated also within the framework of institutional publications as well as on electronic communications networks with particular regard to administrative activities that are carried out for substantial public interest reasons and require no consent by data subjects.

Section 81

(Repealed)

Section 82

(Emergency Situations and Protection of Health and Bodily Integrity)

1. The information referred to in Articles 13 and 14 of the Regulation may be given after the relevant service has been provided, 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. The above information may also be given after the relevant service has been provided, without delay, if any of the following applies:

a) the data subject is physically impaired, legally incapable or unable to distinguish right and wrong, and the information cannot be provided, where so required, to the entity legally representing the data subject, a next of kin, a family member, a person cohabiting with the data subject or registered in a civil union with the latter, a trustee under the terms of Section 4 of Law No 219 of 22 December 2017 or, failing these, the manager of the institution where the data subject is hosted;

b) there exists a serious, impending and irreparable risk to the data subject's health or bodily integrity.

3. The information as per paragraph 1 may also be given after the relevant service has been provided, without delay, if the provision of medical care may be affected - in terms of its timeliness or effectiveness - by the need to make available that information beforehand.

4. Once a person has become of age, the information shall be provided to the data subject if it had not been made available beforehand.

Section 83

(Repealed)

Section 84

(Repealed)

CHAPTER III – PURPOSES IN THE SUBSTANTIAL PUBLIC INTEREST

(Repealed)

Section 86

(Repealed)

CHAPTER IV – MEDICAL PRESCRIPTIONS

(Repealed)

Section 88

(Repealed)

Section 89

(Repealed)

Section 89-a

(Medical prescriptions)

1. Regarding medical prescriptions, special precautions shall be taken by having regard to the provisions made by the Garante in the safeguards referred to in Section 2-f if there is no need to include the data subject's name, partly with a view to checking adequacy of the prescriptions or for administrative purposes or else for scientific research purposes in public health care.

CHAPTER V – GENETIC DATA

(Repealed)

CHAPTER VI – MISCELLANEOUS PROVISIONS

Section 91

(Repealed)

Section 92

(Clinical Records)

1. Where public and private organisations providing health care or welfare services 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 exercise or defend a legal claim in pursuance of Article 9(2), letter f), of the Regulation, such claim being equal in rank to the data subject's right or else consisting in a personal right or another fundamental right or freedom, or

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 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 named 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 named by taking suitable precautions to prevent the latter from being identifiable.

Section 94

(Repealed)

TITLE VI – EDUCATION

CHAPTER I – IN GENERAL

Section 95

(Repealed)

Section 96

(Processing of Data Concerning Students)

1. With a view to facilitating vocational orientation and training as well as occupational inclusion in Italy and abroad, the institutions comprised in the national education system, regional vocational training centres, unrecognised private schools and higher schools for art and performing arts and State universities along with private universities may communicate or disseminate, also to private entities and by electronic networks, 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 those referred to in Articles 9 and 10 of the Regulation, which must be relevant for the above purposes and referred to in the information provided to data subjects pursuant to Article 13 of the Regulation. 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 results by way of a notice to be posted on the school's bulletin board, and those concerning the granting of diplomas and certifications shall be left unprejudiced.

TITLE VII – PROCESSING FOR ARCHIVING PURPOSES IN THE PUBLIC INTEREST, SCIENTIFIC OR HISTORICAL RESEARCH PURPOSES OR STATISTICAL PURPOSES

CHAPTER I – IN GENERAL

Section 97

(Scope of Application)

1. This Title shall regulate processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89 of the Regulation.

Section 98

(Repealed)

Section 99

(Duration of Processing)

1. Processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes may be carried out also for longer than is necessary for achieving the individual 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 archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in compliance with Article 89(1) of the Regulation.

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 are empowered to decide that data concerning studies and researches, graduates, post-graduates, technicians and engineers, researchers, professors, experts and scholars be communicated and disseminated also to private bodies and by electronic networks – except for the data referred to in Articles 9 and 10 of the Regulation.

2. The data subject's rights of rectification, erasure, restriction and objection in pursuance of Articles 16, 17, 18 and 21 of the Regulation shall be left unprejudiced.

3. The data referred to in this Section shall not be regarded as administrative records under the terms of Law 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.

4-a. The rights referred to in paragraph 2 shall be exercised in accordance with the arrangements set out in the rules of conduct.

CHAPTER II – PROCESSING FOR ARCHIVING PURPOSES IN THE PUBLIC INTEREST OR FOR HISTORICAL RESEARCH PURPOSES

Section 101

(Processing Arrangements)

1. No personal data that has been collected for archiving purposes in the public interest or for historical research purposes may be used for taking measures or issuing provisions against the data subject in administrative matters, unless said data are also used for other purposes in compliance with Article 5 of the Regulation.

2. Any document containing personal data that is processed for archiving purposes in the public interest or for historical research 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

(Rules of Conduct Applying to Processing for Archiving Purposes in the Public Interest

or for Historical Research Purposes)

1. The Garante shall encourage adoption of rules of conduct in pursuance of Section 2-c by the private and public entities, including scientific societies and professional associations, that are involved in processing data for archiving purposes in the public interest or historical research purposes.

2. The rules of conduct referred to in paragraph 1 shall set out appropriate safeguards for the rights and freedoms of the data subject, and 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 and the Regulation 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, access to and dissemination of documents concerning data disclosing health, sex life or confidential family-related matters; the cases shall be also specified where either the data subject or an interested party must be informed by the user of the planned dissemination; and

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

Section 103

(Access to Documents Kept in Archives)

1. Access to documents kept in State archives, historical archives of public bodies and private archives that have been declared to be of especially substantial historical interest shall be regulated by legislative decree No 42 of 22 January 2004 and the relevant rules of conduct.

CHAPTER III – PROCESSING FOR STATISTICAL PURPOSES OR SCIENTIFIC RESEARCH PURPOSES

Section 104

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

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

2. For the purpose of implementing this Chapter, account shall be taken with regard to identification data of all the means that can reasonably be used by a 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 purposes or scientific research 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 research purposes shall have to be specified unambiguously and made known to the data subject in accordance with Articles 13 and 14 of the Regulation as also related to Section 106(2), letter b), of this Code and Section 6-a of legislative decree No 322 of 06.09.89 as subsequently amended.

3. Where specific circumstances referred to in the rules of conduct as per Section 106 are such as to allow an entity to respond in the name and 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 purposes or scientific research 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 rules of conduct referred to in Section 106.

Section 106

(Rules of conduct for processing data for statistical purposes or scientific research purposes)

1. The Garante shall encourage the adoption of rules of conduct in pursuance of Section 2-c by the private and public entities, including scientific societies and professional associations, that are involved in processing data for statistical purposes or scientific research purposes with a view to determining appropriate safeguards for the rights and freedoms of the data subject pursuant to Article 89 of the Regulation.

2. Taking account of legislative decree No 322 of 06.09.89 as subsequently amended in respect of the entities that are parties to the National Statistical System and based on similar safeguards in

respect of other entities, the rules of conduct referred to in paragraph 1 shall set out, in particular, the following:

a) the prerequisites and procedures to demonstrate and verify that the data are processed for appropriate statistical purposes or scientific research purposes, except as provided for in the aforementioned legislative decree No 322 of 06.09.89;

b) where not provided for in this Code, further prerequisites for the processing and the respective safeguards as also related to the storage period, 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 reasonably be used by controllers or others in order to identify a data subject whether directly or indirectly, by taking also account of the knowledge acquired in connection with technical developments;

d) the safeguards to be complied with if the data subject's consent is unnecessary, by having regard to the principles laid down in the Recommendations under letter b);

e) simplified arrangements for data subjects to give their consent in connection with processing of the data referred to in Article 9 of the Regulation;

f) the cases where the rights under Articles 15, 16, 18 and 21 of the Regulation may be restricted in accordance with Article 89(2) of the Regulation;

g) the fairness rules applying to collection of the data and the instructions to be addressed to the persons authorised to process the data under the authority of the controller or processor pursuant to Section 2-o ;

h) the measures to be adopted in order to promote compliance with the data minimization principle and the technical and organisational measures referred to in Article 32 of the Regulation, by having also regard to the precautions intended to prevent access by natural persons who are not authorised or designated and the unauthorized identification of data subjects, to the interconnection of information systems also within the framework of the National Statistical System, and to the data exchanges for statistical or scientific research purposes that are carried out with entities and agencies abroad;

i) the commitment by any person authorised to process personal data under the authority of the controller or processor pursuant to Section 2-o to abide by rules of conduct, where such persons are not bound by official or professional secrecy under the law, in order to ensure similar security and confidentiality levels.

Section 107

(Processing of Special Categories of Personal Data)

1. Without prejudice to Section 2-e and except for specific investigations or studies for statistical purposes or scientific research purposes that are provided for by law, the data subject's consent to process the data referred to in Article 9 of the Regulation may be given, where required, in accordance with simplified arrangements as set out in the rules of conduct referred to in Section 106 or in the measures referred to in Section 2-f.

Section 108

(National Statistical System)

1. As well as being subject to the rules of conduct referred to in Section 106(2), 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 with particular regard to processing of the data that are referred to in Article 9 of the Regulation and mentioned in the national statistical programme, provision of information to data subjects, exercise of data subjects' rights and the data falling outside the scope of statistical secrecy under Section 9(4) of the aforementioned decree.

Section 109

(Statistical Data Concerning Births)

1. The collection of statistical data concerning births including malformed newborns and stillborns and the data flows also by healthcare managers 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 to process data relating to health for scientific research purposes in the medical, bio-medical or epidemiological sectors if the said research is carried out in accordance with laws or regulations or EU law pursuant to Article 9(2), letter i), of the Regulation, including research that is part of a bio-medical or health care research programme pursuant to Section 12-a of legislative decree No 502 of 30.12.92, and if a data protection impact assessment is carried out and published in accordance with Articles 35 and 36 of the Regulation. Additionally, consent shall not be necessary if informing the data subjects proves impossible or entails a disproportionate effort on specific grounds, or if it is likely to render impossible or seriously impair the achievement of the research purposes. In such cases, the controller shall take appropriate measures to protect the rights, freedoms and legitimate interests of the data subjects and the research programme shall be the subject of a reasoned, favourable opinion by the geographically competent ethics committee as well as being submitted to the Garante for prior consultation in accordance with Article 36 of the Regulation.

2. Where a data subject exercises his/her rights in pursuance of Article 16 of the Regulation with regard to the processing operations referred to in paragraph 1, any rectification or completion of the data shall be recorded without modifying the data if the rectified or completed data do not produce significant effects on the outcome of the research.

Section 110-a

(Further processing of personal data by third parties for scientific research or statistical purposes)

1. The Garante may authorise further processing of personal data, including the special categories of personal data referred to in Article 9 of the Regulation, for scientific research purposes or statistical purposes by third parties that carry out such activities to a prevailing extent if informing the data subjects proves impossible or entails a disproportionate effort on specific grounds, or if it is likely to render impossible or seriously impair the achievement of the research purposes. In such cases, the controller shall take appropriate measures to protect the rights, freedoms and legitimate interests of the data subjects in accordance with Article 89 of the Regulation including arrangements for the prior minimization and anonymization of the data.
2. The Garante shall communicate the decision adopted on the authorisation request within forty-five days; failing such communication, the request shall be considered to be rejected. When issuing the authorisation or thereafter following checks performed as appropriate, the Garante shall lay down the necessary conditions and measures to ensure adequate safeguards to protect data subjects in connection with the further processing of their personal data by third parties as also related to security issues.
3. Further processing of personal data by third parties for the purposes referred to in this Section may also be authorised by the Garante through decisions of general application to be adopted of its own motion as also related to specific categories of processing and controller. Those decisions shall set out the conditions for further processing and the necessary measures to ensure adequate safeguards to protect data subjects. The decisions adopted pursuant to this paragraph shall be published in the Official Journal of the Italian Republic.
4. Processing for scientific purposes of the personal data collected in the course of clinical activities by public and private *Istituti di ricovero e cura a carattere scientifico* shall not be an instance of further processing by third parties on account of the instrumental nature of the health care activities carried out by such *Istituti* vis-à-vis research activities, subject to compliance with Article 89 of the Regulation.

TITLE VIII – PROCESSING ACTIVITIES IN EMPLOYER-EMPLOYEE RELATIONS

CHAPTER I – IN GENERAL

Section 111

(Rules of conduct for processing activities in employer-employee relations)

1. The Garante shall encourage adoption, pursuant to Section 2-c, of rules of conduct by public and private entities that are involved in processing personal data in employer-employee relationships for the purposes referred to in Article 88 of the Regulation, by also setting forth specific arrangements to inform data subjects.

Section 111-a

(Information regarding received CVs)

1. If an uninvited CV is received with a view to possible recruitment, the information referred to in Article 13 of the Regulation shall be provided when the respective data subject is first contacted thereafter. Within the framework of the purposes referred to in Article 6(1), letter b), of the Regulation, no consent shall be required to process the personal data contained in the CV.

Section 112

(Repealed)

CHAPTER II – PROCESSING OF DATA CONCERNING WORKERS

Section 113

(Data Collection and Relevance)

1. The provisions laid down in Section 8 of Law No 300 of 20 May 1970 and in Section 10 of legislative decree No 276 of 10 December 2003 shall be left unprejudiced.

CHAPTER III – REMOTE SURVEILLANCE, AGILE WORK AND TELEWORK

Section 114

(Safeguards in case of remote surveillance)

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

Section 115

(Telework, agile work and home-based work)

1. In the context of home-based work, telework and agile work, 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 WELFARE BODIES

Section 116

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

1. Assistance boards and welfare bodies 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.

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

TITLE IX – OTHER PROCESSING ACTIVITIES IN THE PUBLIC SECTOR OR IN THE PUBLIC INTEREST

CHAPTER I – INSURANCE COMPANIES

Section 117

(Repealed)

Section 118

(Repealed)

Section 119

(Repealed)

Section 120

(Car Accidents)

1. The Istituto per la vigilanza sulle assicurazioni (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. [7] The provisions contained in Section 135 of the Private Insurance Code as per legislative decree No 209 of 7 September 2005 shall apply to any and all matters that are not regulated by this Section.

TITLE X – ELECTRONIC COMMUNICATIONS

CHAPTER I – ELECTRONIC COMMUNICATIONS SERVICES

Section 121

(Services Concerned and Definitions)

1. This Title shall apply to the processing of personal data in connection with the provision of publicly accessible electronic communications services on public communications networks, including public communications networks supporting data collection and identification devices.[8]

1a. For the purpose of applying the provisions of this Title,

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 contracting party or user receiving the information;

b) 'call' means a connection established by means of a publicly available electronic communications service allowing two-way communication[9];

c) 'electronic communications network' shall mean transmission systems and, where applicable, switching or routing equipment and other resources, including network elements which are not active, which permit the conveyance of signals by wire, radio, 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;[10]

---

[7] 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.
[8] This section was amended by section 1(4) of legislative decree No 69 dated 28 May 2012.
[9] Replaced by Section 1(1)a., No 1, of legislative decree No 69 dated 28 May 2012.
[10] Replaced by Section 1(1)a., No 2, of legislative decree No 69 dated 28 May 2012.

d) ‘public communications network’ shall mean an electronic communications network used wholly or mainly for the provision of publicly available electronic communications services which support the transfer of information between network termination points;[11]

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) ‘contracting party’ 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 contracting party 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 or by an electronic communications service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service;[12]

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.

Section 122

(Information Collected with Regard to Contracting Parties or Users)

1. Storing information, or accessing information that is already stored, in the terminal equipment of a contracting party or user shall only be permitted on condition that the contracting party or user has given his consent after being informed in accordance with simplified arrangements. This shall be without prejudice to technical storage or access to stored information where they are aimed exclusively at carrying out the transmission of a communication on an electronic communications network, or insofar as this is strictly necessary to the provider of an information society service that has been explicitly requested by the contracting party or user to provide the said service. In order to determine the simplified arrangements referred to herein, the Garante shall also take account of the proposals put forward by the nationally most representative consumer and industry associations

[11] Replaced by Section 1(1)a., No 3, of legislative decree No 69 dated 28 May 2012.
[12] Replaced by Section 1(1)a., No 4, of legislative decree No 69 dated 28 May 2012.

involved in order to also ensure that the mechanisms implemented make the contracting party or user actually aware. [13]

2. With a view to giving the consent referred to in paragraph 1 above, specific configurations of software or devices may be used that should be user-friendly as well as unambiguous vis-à-vis the contracting party or user.[14]

2-a. Subject to the provisions made in paragraph 1 above, it shall be prohibited to use an electronic communications network in order to access information stored in the terminal equipment of a contracting party or user, store information, or monitor the operations performed by the user. [15]

Section 123

(Traffic Data)

1. Traffic data relating to contracting parties 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 contracting parties' 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 contracting party or user to whom the data relate has given his/her prior consent. Such consent may be withdrawn at any time.[16]

4. In providing the information referred to in Articles 13 and 14 of the Regulation, the service provider shall inform a contracting party 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 who are authorised to carry out the processing and act directly under the authority of the provider of a publicly available electronic communications service or, where applicable, the provider of a public communications network, in pursuance of Section 2-c, and who 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 authorised person accessing the data, also by means of automated search procedures.

---

[13] This paragraph was replaced by section 1(5)a. of legislative decree No 69 dated 28 May 2012.
[14] This paragraph was replaced by section 1(5)b. of legislative decree No 69 dated 28 May 2012.
[15] This paragraph was added by section 1(5)c. of legislative decree No 69 dated 28 May 2012.
[16] This paragraph was amended by section 1(6) of legislative decree No 69 dated 28 May 2012.

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. Contracting parties 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 contracting parties concerning the communications performed.

4. The final three digits of the called numbers shall not be displayed in contracting parties' bills. A contracting party 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 contracting party must have the same possibility on a per-line basis. The provisions set out in Section 2(1) of Law No 5 of 11 January 2018 shall be left unprejudiced.

2. Where presentation of calling line identification is available, the provider of a publicly available electronic communications service shall ensure that the called contracting party 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 contracting party 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 contracting party.

4. Where presentation of connected line identification is available, the provider of a publicly available electronic communications service shall ensure that the called contracting party 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 contracting parties 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 contracting parties 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 contracting parties, 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 contracting parties, 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 contracting parties has been obtained for the processing of location data other than traffic data, the user or contracting party 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 authorised to carry out the processing in pursuance of Section 2-p who act 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 authorised persons accessing the data also by means of automated search operations.

Section 127

(Nuisance and Emergency Calls)

1. Any contracting party 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 contracting party 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 contracting party 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 contracting parties 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 contracting party 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 contracting party, free of charge and using simple means, to stop automatic call forwarding by third parties to his/her own terminal.

Section 129

(Directories of Contracting Parties)

1. The Garante shall determine, in co-operation with the Authority for Communications Safeguards as per Section 154(4) as well as in compliance with EU law, the arrangements for entering and subsequently using contracting parties' personal data in publicly available paper or electronic directories.

2. The determination referred to in Section 1 shall lay down appropriate mechanisms for contracting parties to give their consent to inclusion in said directories as well as to the use of their data for the purposes of sending advertising materials, direct selling, marketing surveys or marketing communications as well as for the purposes referred to in Article 21(2) of the Regulation, whereby the applicable principles shall consist in the highest possible simplification of the arrangements for inclusion in a directory that is only intended to allow searching the contact details of a contracting party for person-to-person communications, and in obtaining the contracting party's express, specific consent if the processing is carried out for purposes other than those mentioned

above. Furthermore, the mechanisms for the contracting parties to access, rectify or erase their data free of charge shall also be set out.

Section 130

(Unsolicited Communications)

1. Without prejudice to the provisions made in sections 8 and 21 of legislative decree No 70 dated 9 April 2003, the use of automated calling or communications 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 contracting party's or user's consent.[17] The provisions made in Section 1(14) of Law No 5 of 11 January 2018 shall be left unprejudiced.

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 Articles 6 and 7 of the Regulation as well as under the terms of paragraph 3-a below[18].

3-a. By way of derogation from Section 129, processing by telephone and mail of the data referred to in paragraph 1 of the aforementioned Section for the purposes of sending advertising materials, direct selling, marketing surveys or marketing communications 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.[19] [Amended by Section 6(2)a, item 6. of decree No 70 dated 13 May 2011]

3-b. The register as per paragraph 3-a shall be set up by a decree of the President of the Republic to be adopted in pursuance of section 17(2) of Law 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

---

[17] This paragraph was amended by Section 1(7)a, nos. 1, 2 and 3, of legislative decree No 69 dated 28 May 2012.
[18] This paragraph was amended by Section 20-a, paragraph 1, letter a., of the decree No 135 dated 25 September 2009, as converted with amendments into Law No 166 dated 20 November 2009.
[19] This paragraph along with paragraph 3-b and paragraph 3-c was added by Section 20-bis, paragraph 1, letter b., of the decree No 135 dated 25 September 2009, as converted with amendments into Law No 166 dated 20 November 2009. For the sake of completeness, paragraphs 2 to 4 of Section 20-a of the aforementioned decree are reported below:
"2. The register mentioned in Section 130(3-a) 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] Law. 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-a) of decree No 207 dated 30 December 2008 as converted, with amendments, into Law 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 Law 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."

– 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 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 referred to in legislative decree No 50 of 18 April 2016. 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 of sending advertising materials, direct selling, marketing surveys or marketing communications 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 Articles 6 and 7 of the Regulation.

3-b. 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 in breach of section 8 of legislative decree No 70 dated 9 April 2003, or without a valid address to which the data subject may send a request to exercise the rights referred to in Articles 15 to 22 of

the Regulation, or by encouraging recipients to visit websites that contravene the said section 8 of legislative decree No 70/2003, shall be prohibited.[20]

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 Article 58 of the Regulation, 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 Contracting Parties and Users)

1. The provider of a publicly available electronic communications service shall inform contracting parties 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. Contracting parties 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 contracting parties' premises.

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

[20] This paragraph was amended by Section 1(7)b., nos. 1 and 2, of legislative decree No 69 dated 28 May 2012.

Section 132[21] [22]

(Traffic Data Retention for Other Purposes)

1. [23] 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.

---

[21] As amended by Decree-Law No 354 of 24th December 2003, converted, with amendments, into Law No 45 of 26th February 2004; Decree-Law No 144 of July 27, 2005 converted with amendments into Law No 155 of July 31, 2005 ("Urgent Measures to Fight Terrorism"), Decree-Law No 248/2007 converted with amendments into Law No 31/2008 dated 27 February 2008, Law 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 Law 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."

[22] As for the retention of telephone and Internet traffic data, reference should also be made to Section 4a of legislative decree No 7 of 18 February 2015 as enacted, including amendments thereof, by Law No 43 of 17 April 2015 and subsequently amended by decree No 210 of 30 December 2015 as enacted, including amendments thereof, by Law No 21 of 25 February 2016. The text of the said Section is reported below:
'Section 4a. Provisions on the Retention of Telephone and Internet Traffic Data. – 1. By way of derogation from the provisions made in Section 132(1) of the Code referred to in legislative decree No 196 of 30 June 2003 as amended thereafter, the telephone and Internet traffic data – except for the contents of communications – that are held by telecommunication service operators as of the date of entry into force of the Law enacting this decree along with the data of telephone and Internet traffic occurring thereafter shall be retained until 30 June 2017 for the purposes of detection and suppression of the criminal offences mentioned in Sections 51(3c) and 407(2), letter a), of the Criminal Procedure Code. – 2. The data relating to the unsuccessful calls made as from the date of entry into force of the Law enacting this decree, which are processed on a temporary basis by the providers of publicly available electronic communications services or public communication networks, shall be retained until 30 June 2017. – 3. The provisions under paragraphs 1 and 2 above shall no longer apply as from 1 July 2017.'

[23] 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.

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.[24]

2. [Repealed.] [25]

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 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-c of the Criminal Procedure Code. The request for direct access to incoming telephone calls may only be made if the latter are likely to factually, effectively affect the performance of defence investigations as per Law No 397 of 7 December 2000. If that is not the case, the rights referred to in Articles 12 to 22 of the Regulation may be exercised in accordance with the mechanisms mentioned in Section 2-m(3), third, fourth and fifth paragraph.

4. [Repealed.]

4-a. [Repealed.]

4-b.[26] 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-c. 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-d. The measures taken under paragraph 4-b 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

[24] 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.
[25] This paragraph was repealed by Section 2(1)c. of legislative decree No 109/2008 along with paragraph 4 and paragraph 4-bis hereof..
[26] This paragraph was added by Section 10 of Law No 48 dated 10 March 2008 along with paragraph 4-quater and 4-quinquies hereof.

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. [27] 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 by the Garante pursuant to the arrangements set out in Section 2-p, which are aimed at ensuring that the retained data meet the same quality, security and protection requirements as network data as well as at [28]laying down technical mechanisms to regularly destroy the data after expiry of the term referred to in paragraph 1.

5-a. The provisions laid down in Section 24 of Law No 167 of 20 November 2017 shall be left unprejudiced.

Section 132-a[29]

(Procedures Set out by Providers)

1. Providers shall set out internal procedures to meet the requests made in compliance with the provisions that envisage access to users' personal data.

2. Upon request, providers shall provide the Garante, having regard to the respective scope of competence, with information on the procedures referred to in paragraph 1, the number of requests received, the legal justification invoked and their response.

Section 132-b

(Security of processing)

1. In accordance with Article 32 of the Regulation, providers of publicly available electronic communications services shall be subject to this Section.
2. Providers of publicly available electronic communications services shall take technical and organisational measures that are appropriate in the light of the existing risk under the terms of Article 32 of the Regulation; to that effect, they may rely on other entities that have been entrusted with providing the given service.
3. Any entity operating on electronic communications networks shall ensure that personal data are only accessible to authorised staff for legally permitted purposes.
4. The measures referred to in paragraphs 2 and 3 shall ensure the protection of traffic and location data and of any other personal data that is stored or transmitted against destruction, accidental or otherwise, loss or alteration, accidental or otherwise, and against unauthorised or unlawful storage, archiving, access or disclosure; such measures shall also ensure implementation of a security policy.
5. If security of the service or the personal data requires taking measures that concern 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 to that effect, the dispute shall be settled by the Authority for Communications

[27] This paragraph had been amended by Section 2(1)d. of legislative decree No 109/2008.
[28] This letter had been amended by Section 2(1)d., point 3, of legislative decree No 109/2008.
[29] This section was added by Section 1(8) of legislative decree No 69 dated 28 May 2012.

Safeguards upon the request of either provider in accordance with the arrangements that are envisaged in the legislation in force.

Section 132-c

(Information on risks)

1. The provider of a publicly available electronic communications service shall inform subscribers and, where possible, users, using clear language that is appropriate and suitable by having regard to age and category of the data subject receiving such information and taking special care in case children are involved, whether there is a particular risk of network security breach; if that risk falls outside the scope of application of the measures the provider is required to take pursuant to Section 132-b, paragraphs 2, 3 and 5, the provider shall specify all the possible remedies and the expected costs. Similar information shall be provided to the Garante and the Authority for Communications Safeguards.

CHAPTER II – INTERNET AND ELECTRONIC NETWORKS

(Repealed)

CHAPTER III – VIDEO SURVEILLANCE

(Repealed)

TITLE XI – SELF-EMPLOYED PROFESSIONALS AND PRIVATE DETECTIVES

(Repealed)

TITLE XII – JOURNALISM, FREEDOM OF EXPRESSION AND INFORMATION

CHAPTER I – IN GENERAL

Section 136

(Journalistic Purposes and Other Intellectual Works)

1. This Title shall apply in pursuance of Article 85 of the Regulation 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 Law No 69 of 03.02.63; or

c) that are aimed exclusively at publishing or circulating, also occasionally, articles, essays and other intellectual works also in terms of academic, artistic or literary expression.

Section 137

(Applicable Provisions)

1. With regard to the provisions made in Section 136, the data referred to in Articles 9 and 10 of the Regulation may be processed also without the data subject's consent providing the rules of conduct mentioned in Section 139 are abided by.

2. The processing activities referred to in Section 136 shall not be subject to the following:
a) The safeguards referred to in Section 2-f and the decisions of general application referred to in Section 2-p;
b) The provisions contained in Chapter V of the Regulation concerning transfers of personal data to third countries or international organisations.

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 Article 1(2) of the Regulation and Section 1 of this Code, in particular the essential nature 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 data subject'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 Article 15(1), letter g), of the Regulation.

CHAPTER II – RULES OF CONDUCT CONCERNING JOURNALISTIC ACTIVITIES

Section 139

(Rules of Conduct Concerning Journalistic Activities)

1. The Garante shall encourage, pursuant to Section 2-c, adoption of rules of conduct concerning processing of the data as per Section 136 by the National Council of the Press Association. The rules shall lay down measures and arrangements to safeguard data subjects as appropriate in respect of the nature of the data, with particular regard to the data relating to health and sex life or sexual orientation. The rules may also lay down specific arrangements for providing the information referred to in Articles 13 and 14 of the Regulation.
2. The rules of conduct and any amendments or additions to those rules that fail to be adopted by the National Council within six months of the proposal put forward by the Garante shall be adopted by the Garante and be effective until different rules come into force pursuant to the cooperation procedure.
3. The rules of conduct and any amendments or additions thereto shall come into force fifteen days after publication in the Official Journal of the Italian Republic in pursuance of Section 2-c.
4. Should any of the provisions in the rules of conduct be infringed, the Garante may prohibit the processing pursuant to Article 58 of the Regulation.
5. The Garante shall lay down measures and arrangements to safeguard data subjects in cooperation with the National Council of the Press Association; the National Council shall be required to implement such measures and arrangements.

TITLE XIII – DIRECT MARKETING

CHAPTER I – IN GENERAL

Section 140

(Repealed)

PART III – REMEDIES AND SANCTIONS

TITLE I – ADMINISTRATIVE AND JUDICIAL REMEDIES

CHAPTER 0.I – MUTUALLY ALTERNATIVE MEANS OF REDRESS

Section 140-a

(Mutually Alternative Means of Redress)

1. A data subject may lodge a complaint with the Garante or bring a proceeding before a judicial authority where he or she believes that any of the rights afforded by the legislation on personal data protection have been infringed.
2. A complaint with the Garante may not be lodged if a proceeding has already been brought before a judicial authority by the same parties and with regard to the same subject matter.
3. Lodging a complaint with the Garante shall prevent bringing an additional proceeding before a judicial authority by the same parties and with regard to the same subject matter, except as provided for in Section 10(4) of legislative decree No 150 of 1 September 2011.

CHAPTER I – REMEDIES AVAILABLE TO DATA SUBJECTS BEFORE THE GARANTE

Section 141

(Complaint with the Garante)

1. A data subject may lodge a complaint with the Garante in accordance with Article 77 of the Regulation.

Section 142

(Lodging a Complaint with the Garante)

1. The complaint shall specify, in as detailed a manner as possible, the underlying facts and circumstances, the allegedly infringed provisions and the remedies sought and shall contain the identification data concerning the controller and the processor, if known.
2. The complaint shall be undersigned either by the data subject or by a non-profit body regulated by legislative decree No 117 of 3 July 2017, acting under the data subject's mandate, which must be active in the field of the protection of data subjects' rights and freedoms with regard to the protection of personal data.
3. Such documents as may be helpful for assessment purposes shall be attached to the complaint along with the mandate given by the data subject, if any; an address for sending any communications, including via emails, facsimile or telephone, shall be also specified.

4. The Garante shall make available a complaint form and publish it on its institutional website; dissemination of the form in electronic format shall be promoted.
5. The Garante shall set out the procedure for handling complaints in its own rules of procedure and may provide for simplified arrangements and shorter deadlines in respect of the handling of complaints concerning alleged infringements of Articles 15 to 22 of the Regulation.

Section 143

(Handling of Complaints)

1. Having concluded the preparatory phase, the Garante may take the measures referred to in Article 58 of the Regulation in accordance with the provisions made in Article 56 thereof if the complaint is found not to be clearly unsubstantiated and the prerequisites for a decision on the complaint are fulfilled, also prior to finalising the relevant proceeding.
2. The measures referred to in paragraph 1 shall be published in the Official Journal of the Italian Republic if the respective addressees cannot be identified easily because of their number or else on account of the complex investigations carried out.
3. The Garante shall decide on a complaint within nine months of the date the complaint was lodged and shall inform the data subject on the progress of the complaint within three months of the said date. Where there are reasons related to the preparatory activities, which the Garante shall communicate to the data subject, the decision on a complaint shall be made within twelve months of the aforementioned date. If the cooperation procedure envisaged in Article 60 of the Regulation is initiated, the running of time shall be stopped for as long as the said procedure is in progress.
4. The decision may be challenged before a judicial authority pursuant to Section 152.

Section 144

(Reports)

1. Anyone may submit a report, which the Garante may take into consideration also with a view to taking any of the measures referred to in Article 58 of the Regulation.

III – NON-JUDICIAL REMEDIES

Section 145

(Repealed)

Section 146

(Repealed)

Section 147

(Repealed)

Section 148

(Repealed)

Section 149

(Repealed)

Section 150

(Repealed)

Section 151

(Repealed)

CHAPTER II – JUDICIAL REMEDIES

Section 152

(Judicial Authorities)

1. Competence over any disputes concerning the matters addressed in the judicial proceedings referred to in Articles 78 and 79 of the Regulation as well as in proceedings relating to application of personal data protection legislation or the right to compensation pursuant to Article 82 of the said Regulation shall lie with judicial authorities.[30]

1-bis. Any disputes as per paragraph 1 shall be regulated by section 10 of legislative decree No 150 of 1 September 2011. [31]

---

[30] This paragraph was amended by section 34(9)a. of decree No 150/2011 subject to the applicability limitations set forth in section 36 of the said decree.

[31] This paragraph was added by section 34(9)b. of decree No 150/2011 subject to the applicability limitations set forth in section 36 of the said decree.
For the sake of completeness, the text of section 10 of legislative decree No 150/2011 is reported below in full:

Section 10 – Disputes concerning application of the provisions contained in the Personal Data Protection Code

2. [Repealed][32]

3. [Repealed]

4. [Repealed]

5. [Repealed]

6. [Repealed]

7. [Repealed]

8. [Repealed]

9. [Repealed]

10. [Repealed]

11. [Repealed]

12. [Repealed]

13. [Repealed]

14. [Repealed]

---

1. Any disputes as per section 152 of legislative decree No 196 dated 30 June 2003 shall be regulated in accordance with the procedural arrangements applying to cases on employer-employee relationships except where provided otherwise in this section.
2. Jurisdiction shall lie with the court of the place where the data controller is resident pursuant to the definitions contained in section 4 of legislative decree No 196 dated 30 June 2003.
3. Under penalty of inadmissibility, any provision by the Italian data protection authority shall be challenged by filing a petition within thirty days as from the date on which the said provision was notified or the relevant complaint was tacitly dismissed; the deadline shall be sixty days if the petition is filed by an entity residing abroad.
4. Enforcement of a provision that has been challenged may be staid in accordance with section 5.
5. Should the petitioner fail to appear on the first day in court without alleging any legitimate impediment, the judge shall order that the case be struck off the list and declare that the relevant proceeding is extinguished, and also award legal costs to the petitioner.
6. The judgment issued by the court may not be appealed and may order that the necessary measures be taken partly by derogating from the prohibition set forth in section 4 of Law No 2248 dated 20 March 1865, Annex E, as also related to any acts by public bodies in their capacity as either data controllers or data processors, and may award damages.

[32] This paragraph along with the subsequent ones were repealed by section 34(9)c. of legislative decree No 150/2011. See the provisions made in section 36 of the latter decree.

TITLE II – INDEPENDENT SUPERVISORY AUTHORITY

CHAPTER I – THE GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Section 153

(The Garante per la protezione dei dati personali)

1. The Garante shall be composed of the Panel of Commissioners, which shall be the head thereof, and the Bureau. The Panel of Commissioners shall include 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 elected out of the candidates applying to a selection procedure to be publicised by a notice posted on the websites of the Chamber of Deputies, the Senate and the Garante at least sixty days prior to the respective appointments. The applications shall be sent in no later than thirty days prior to the appointment and the relevant CVs shall be published in the said websites. Applicants shall be persons ensuring independence with proven experience in the field of personal data protection with particular regard to law or computer science.
2. The members shall elect a President from amongst themselves; the President shall have the casting vote in the case of a tie. The members shall also elect a Vice-President, who shall replace the President if the latter is absent or unable to discharge his or her functions.
3. [33] President and members shall hold office for seven years; their term of office shall not be renewable. For the duration of their terms, President and members shall not be allowed - under penalty of disqualification - to carry out professional or advisory activities, whether gainful or not, be managers or employees of public or private entities or hold elective offices.
4. The members of the Panel of Commissioners shall keep secret, both during and after their term of office, any confidential information they may have acquired in discharging their functions or exercising their powers.
5. Upon accepting their appointment, the President and members shall be struck off the list of permanent staff if they are employees in the public administration or practising members of the judiciary; if they are faculty professors at an University, they shall be put on leave of absence with no wages pursuant to Section 13 of Presidential decree No 382 of 11.07.1980. The employees who have been struck off the list of permanent staff or put on leave of absence may not be replaced.
6. The President shall be entitled to an allowance not exceeding the salary paid to the President of the Court of Cassation (*Corte di Cassazione*) subject to the restrictions that are envisaged by law in respect of the total annual income of any individual receiving sums or salaries paid from public money in connection with his or her work, whether as an employee or as a self-employed professional, for governmental organisations. Members shall be entitled to an allowance not exceeding two-thirds of the one granted to the President.
7. The Bureau referred to in Section 155 shall be placed under the authority of the Garante.

[33] This paragraph was amended by section 47-c of Law 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.

8. President, members, secretary general and staff shall refrain from handling proceedings before the Garante for two years following termination of their functions or service with the Garante, including the submission of complaints, requests for opinions or queries on behalf of third parties.

Section 154

(Tasks)

1. In addition to the provisions made in specific pieces of legislation as well as in Section II of Chapter VI of the Regulation and pursuant to Article 57(1), letter v) of the said Regulation, the Garante shall, also of its own motion and by relying on the Bureau, in accordance with the applicable legislation as well as in respect of one or more than one controller:

a) verify whether data processing operations are carried out in compliance with applicable laws and regulations, also in case of termination of processing and with regard to the storage of traffic data[34];

b) handle the complaints lodged with it in pursuance of the Regulation and the provisions of this Code, by also laying down specific arrangements in that respect through its rules of procedure and setting the priority issues as resulting annually from such complaints, which issues may then become the subject of investigations in the course of the relevant year;

c) encourage the adoption of rules of conduct in the cases mentioned under Section 2-c;

d) report facts and/or circumstances amounting to offences to be prosecuted ex officio, which it has come to know either in carrying out or on account of its functions;

e) transmit the annual report as drawn up pursuant to Article 59 of the Regulation to Parliament and Government by the 31st of May of the year following that to which the report refers;

f) ensure the protection of the fundamental rights and freedoms of the individuals by implementing the Regulation and this Code as appropriate;

g) discharge such tasks as are allocated to it by Union or State law and carry out such additional functions as are laid down in domestic law.

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

a) Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II) and Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II);
b) Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA;
c) Regulation (EU) 2015/1525 of the European Parliament and of the Council of 9 September 2015 amending Council Regulation (EC) No 515/97 on mutual assistance between the administrative authorities of the Member States and cooperation between

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

the latter and the Commission to ensure the correct application of the law on customs and agricultural matters and Council Decision 2009/917/JHA of 30 November 2009 on the use of information technology for customs purposes;

d) Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice;

e) Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation) and Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences;

f) Regulation (EU) No 1024/2012 of the European Parliament and of the Council of 25 October 2012 on administrative cooperation through the Internal Market Information System and repealing Commission Decision 2008/49/EC ('the IMI Regulation');

g) 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 Law 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. Regarding any matters that are not addressed in the Regulation or this Code, the Garante shall regulate, by way of its own rules of procedure in pursuance of Section 156(3) hereof, the specific arrangements for any proceedings related to discharge of the tasks or exercise of the powers conferred on it by the Regulation or this Code.
4. The Garante shall co-operate with other national independent administrative authorities in discharging the respective tasks.
5. Subject to such shorter terms as may be provided for by law, the Garante's opinion shall be rendered within forty-five days of receiving the relevant request, including the requests referred to in Article 36(4) of the Regulation. Upon expiry of that 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 from the administrative agencies concerned for preparation of the case.
6. A copy of any measure taken by judicial authorities in connection with either this Code or computer crimes shall be transmitted to the Garante by the court clerk's office.
7. The Garante shall not be competent for supervision over processing that is carried out by judicial authorities acting in their judicial capacity.

Section 154-a

(*Powers*)

1. In addition to the provisions made in specific pieces of legislation, in Section II of Chapter VI of the Regulation, and in this Code, the Garante shall be empowered pursuant to Article 58(6) of the Regulation to:
   a) Adopt guidance concerning the technical and organisational measures to implement the principles of the Regulation, also with regard to individual sectors and in pursuance of the principles set out in Article 25 of the Regulation;
   b) Approve the rules of conduct referred to in Section 2-c.

2. The Garante may invite representatives of other national independent administrative authorities to participate in its meetings or be invited to the meetings held by other national independent administrative authorities and take part in discussing issues of shared interest; the Garante may also request the cooperation of specialised staff from any other national independent administrative authority.
3. The Garante shall publish its decisions based on the provisions made in an instrument of general application regulating the duration of such publication, the publication in the Official Journal of the Italian Republic and on the Garante's own website, and the cases where it is empowered to blank certain items in its decisions.
4. Having regard to the simplification requirements applying to SMEs as defined in Recommendation 2003/361/EC, the Garante shall promote, in compliance with the provisions contained in the Regulation and in this Code, simplified arrangements to fulfil the obligations placed on controllers by way of the guidance adopted under paragraph 1, letter a), above.

Section 154-b

(*Power to commence legal proceedings and legal representation)*

1. The Garante shall be empowered to commence legal proceedings against a controller or processor in case of infringement of personal data protection provisions.
2. The Garante shall be represented in judicial proceedings by the Avvocatura dello Stato in pursuance of section 1 of Royal Decree No 1611 of 30 October 1933.
3. Should a conflict of interests arise, the Garante may stay in court, having consulted with the Avvocato Generale dello Stato, by the agency of its own officials who shall be included in the special list of lawyers working as employees of public bodies, or else by the agency of any lawyer practicing as a self-employed professional.

CHAPTER II - THE BUREAU

Section 155

(The Bureau)

1. In order to ensure accountability and autonomy pursuant to Law No 241 of 07.08.90, as subsequently amended, and legislative decree No 29 of 03.02.93, as subsequently amended, the Bureau of the Garante shall implement the principles concerning appointment and tasks of officials responsible for handling the individual cases and separation between guidance and supervisory tasks as committed to the heads of the authority and managerial tasks as committed to the heads of departments or units. The provisions of legislative decree No 165/2001 shall also apply insofar as they are expressly referred to in this Code.

Section 156

(List of Permanent Staff and Provisions Concerning Human Resources)

1. The Bureau of the Garante shall be under the authority of a secretary general, who shall be appointed out of individuals with proven high-level qualifications as related to the position covered and the objectives to be achieved and may be selected from the ranks of the judiciary, including administrative courts and courts of auditors, *avvocati di Stato* [State lawyers defending public bodies and employees in administrative law proceedings], full professors in law and economics, and senior heads of departments in public bodies.

2. The list of permanent staff shall include 162 positions. The list of permanent staff may only be joined following a public competitive examination. Where this is considered helpful with a view to ensuring cost-effectiveness and efficiency of administrative activities and in order to foster the recruitment of more experienced staff in connection with the public competitive examination procedures referred to in the second sentence hereof, the Garante may reserve no more than fifty percent of the vacancies to be filled through such procedures to permanent staff of public administrative bodies that have been recruited via public competitive examinations and have held their positions for at least three years. Section 30 of legislative decree No 165 of 30 March 2001 shall only apply in respect of the permanent staff of the independent administrative authorities referred to in decree-law No 90 of 24 June 2014 as subsequently enacted, including the amendments thereof, by Law No 114 of 11 August 2014.

3. The Garante shall set out the following by way of own rules of procedure to be published in the Official Journal of the Italian Republic:

a) organisation and operation of the Bureau also with a view to discharging the tasks and exercising the powers referred to in Sections 154, 154-a, and 160 hereof and in Article 57(1) of the Regulation;

b) career paths and recruitment of staff in pursuance of the principles and procedures referred to in Sections 1, 35 and 36 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 Law No 249 of 31.07.97 as subsequently amended and, in respect of heads of department, Section 19(6) and 23-a 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; and

e) administration and accounting mechanisms, also by derogating from the provisions applying to State accounts.

4. Personnel from the State's civil service, other public administrative bodies or public entities in general may be employed by the Bureau for specified reasons. No more than twenty positions may be covered in this manner, of which positions no more than twenty percent shall be heads of department. Such personnel shall be either struck off the list of permanent staff or placed on equal terms with the Bureau's staff in accordance with the respective regulations; alternatively, they shall be put on leave of absence pursuant to Section 13 of Presidential Decree No 382 of 11.07.80 as subsequently amended. A corresponding number of vacancies shall be left available in the relevant permanent lists.

5. In addition to the list of permanent staff, the Bureau may directly recruit employees on the basis of time-limited contracts or hire consultants pursuant to Section 7(6) of legislative decree No 165/2001; the total number of such employees and consultants shall not be in excess of twenty. Section 36 of legislative decree No 165/2001 shall be left unprejudiced as regards time-limited contracts.

6. Staff and consultants working for the Bureau shall be subject to a duty of secrecy both during and after their period of employment with regard to any confidential information which has come to their knowledge in the course of the performance of their tasks.

7. The staff from the Bureau in charge of the investigations referred to in Section 158 hereof and in Articles 57(1), letter h), 58(1), letter b), and 62 of the Regulation shall act in the capacity of judicial police officers or staff as related to the duties they are required to fulfil in accordance with the powers respectively conferred on them.

8. Pursuant to Article 52(4) of the Regulation, the operating costs concerning the Garante including such expenses as may be necessary to ensure participation in the cooperation and consistency procedures as introduced by the Regulation and those relating to the human, technical and financial resources, premises and facilities required to effectively perform its tasks and exercise the relevant powers shall be covered by ad-hoc appropriations made in the State budget and included as specific items in the mission and expenditures of the Ministry of Economy and Finance. The accounting statements shall be audited by the State Auditors' Department (*Corte dei Conti*). The Garante may request the controller to pay handling fees in connection with specific proceedings.

CHAPTER III - INQUIRIES AND CONTROLS

Section 157

(Request for Information and Provision of Documents)

1. Within the framework of the powers set out in Article 58 of the Regulation and in order to discharge its tasks, the Garante may request the controller, the processor, the controller's or processor's representative, the data subject or a third party to provide information and produce documents as also related to the contents of databases.

Section 158

(Inquiries)

1. The Garante may order that databases and filing systems be accessed and other inspections or checks be carried out at the premises where the processing takes place or investigations are to be performed that are instrumental on whatever ground to check compliance with personal data protection law.

2. The inquiries referred to in paragraph 1 and the investigations carried out in pursuance of Article 62 of the Regulation shall be carried out by staff from the Bureau; members or staff from the supervisory authorities of other EU Member States may participate where appropriate.

3. The Garante may also avail itself, if necessary, of the co-operation of other State agencies in discharging its institutional tasks.

4. Where the inquiries referred to in paragraphs 1 and 2 are carried out at a person's home or in another private dwelling place and/or the relevant appurtenances, the controller's or processor's informed consent shall be required. Alternatively, an authorisation shall be required from the judge presiding over the court that is competent geographically for the place where the inquiries are to be carried out, and such authorisation shall be granted by a reasoned decree without delay and anyhow within three days of receiving the relevant request from the Garante if it can be proven that the inquiries cannot be postponed.

5. Subject to the safeguards referred to in paragraph 4, the inquiries carried out at the places mentioned therein may also concern publicly available communications networks and entail the online acquisition of data and information. To that end, specific minutes shall be drawn whilst ensuring the right of every party to be heard if the said inquiries are carried out at the controller's.

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 Section 58, 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 the Regulation or 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 in respect of any information that has to remain confidential. 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 and, where this is necessary for the discharge of official duties, to a limited number of employees in the Office to be designated by the Garante pursuant to criteria laid down in the regulations referred to in Section 156(3), letter a).

4. As for inquiries mentioned in paragraph 3 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.

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.

Section 160-a

(Validity, enforceability and admissibility in judicial proceedings of records, documents and measures based on processing of personal data that is not compliant with laws or the Regulation)

1. Validity, enforceability and admissibility in judicial proceedings of records, documents and measures based on processing of personal data that is not compliant with laws or the Regulation shall continue to be regulated by the relevant procedural law provisions.

TITLE III - PENALTIES

CHAPTER I - BREACH OF ADMINISTRATIVE RULES

Section 161

(Providing No or Inadequate Information to Data Subjects)

(Repealed)

Section 162

(Other Types of Non-Compliance)

(Repealed)

Section 162-bis

(Penalties Applying to Traffic Data Retention)

(Repealed)

Section 162-ter

(Penalties against Providers of Publicly Available Electronic Communications Services)

(Repealed)

Section 163

(Failure to Submit Notification or Submitting an Incomplete Notification)

(Repealed)

Section 164

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

(Repealed)

Section 164-bis

(Less Serious Cases and Aggravating Circumstances)

(Repealed)

Section 165

(Publication of Provisions by the Garante)

(Repealed)

Section 166

(Criteria for applying administrative fines and procedure for adopting corrective measures and sanctions)

1. Any violation of the provisions referred to in Section 2-d, paragraph 2, Section 2-p, Section 92(1), Section 93(1), Section 123(4), Section 128, Section 129(2) and Section 132-b shall entail the imposition of an administrative fine pursuant to Article 83(4) of the Regulation.

An administrative fine shall also be imposed on any entity that fails to carry out the impact assessment referred to in Section 110(1), first sentence, or that fails to submit the research programme to the Garante's prior consultation in accordance with the third sentence of Section 110(1).

2. Any violation of the provisions referred to in Section 2-b, Section 2-d, paragraph 1, Section 2-e, Section 2-f, paragraph 8, Section 2-g, Section 2-n, paragraphs 1 to 4, Section 52, paragraphs 4 and 5, Section 75, Section 78, Section 79, Section 80, Section 82, Section 92(2), Section 93, paragraphs 2 and 3, Section 96, Section 99, Section 100, paragraphs 1, 2 and 4, Section 101, Section 105, paragraphs 1, 2 and 4, Section 110-a, paragraphs 2 and 3, Section 111, Section 111-a, Section 116, paragraph 1, Section 120, paragraph 2, Section 122, Section 123, paragraphs 1, 2, 3 and 5, Section 124, Section 125, Section 126, Section 130, paragraphs 1 to 5, Section 131, Section 132, Section 132-a, paragraph 2, Section 132-c, Section 157, and of the safeguards and rules of conduct referred to in Section 2-f and 2-c, respectively, shall entail the imposition of an administrative fine pursuant to Article 83(5) of the Regulation.
3. The Garante shall be empowered to adopt the corrective measures referred to in Article 58(2) of the Regulation and to impose the administrative fines referred to in Section 83 of the said Regulation and in paragraphs 1 and 2 hereof.
4. The proceeding to adopt the measures and fines referred to in paragraph 3 may be initiated against both private and public bodies or public authorities following a complaint lodged in accordance with Article 77 of the Regulation or else following inquiries carried out by the Garante of its own motion, within the framework of the exercise of the investigative powers referred to in Article 58(1) of the Regulation as well as in connection with accesses, inspections and audits that are carried out on the basis of either autonomous powers to carry out controls or of powers delegated by the Garante.
5. Where the Bureau considers that the findings of the activities referred to in paragraph 4 indicate the commission of one or more of the violations mentioned in this Title and in Article 83, paragraphs 4 to 6, of the Regulation, it shall start the proceeding to adopt the measures and fines referred to in paragraph 3 hereof by notifying the controller or the processor of the alleged violations in accordance with the safeguards set out in the Regulations referred to in paragraph 9 hereof, except where the prior notification of such alleged violations proves incompatible with the nature and objective of the measures to be adopted.
6. Within thirty days of receiving the communication referred to in paragraph 5, the entity that has committed the alleged violations may send pleadings or documents to the Garante and may request to be heard by the Garante.
7. Sections 1 to 9, 18 to 22, and 24 to 28 of Law No 689 of 24 November 1981 shall be complied with, where applicable, in adopting the administrative fines referred to in paragraph 3. In such cases the ancillary administrative sanction may be imposed consisting in publication of the injunctive order, in part or as a whole, on the Garante's website. Fifty percent of the total annual proceeds from the administrative fines shall be fed into the appropriations mentioned in Section 156(8), being intended for the specific awareness-raising and inspection activities as well as for the implementation of the Regulation carried out by the Garante.
8. Within the deadline for challenging the Garante's order as mentioned in Section 10(3) of legislative decree No 150/2011, the entity that has committed the violation and those jointly and severally liable therefor may settle the litigation by complying with the measures imposed by the Garante, if any, and paying half of the amount of the administrative fine imposed by the Garante.
9. The Garante shall lay down the procedure for adopting the measures and administrative fines referred to in paragraph 3 along with the respective deadlines in regulations of its own

to be published in the Official Journal of the Italian Republic, in accordance with Article 58(4) of the Regulation and by respecting the principles of full disclosure of procedural documents, equality of arms, full reporting, and separation between preparatory and decision-making phase in imposing any administrative fine.

10. The provisions on administrative fines as set out in this Code and Article 83 of the Regulation shall not apply to processing activities in the judicial sector.

CHAPTER II - CRIMINAL OFFENCES

Section 167

(Unlawful Data Processing)

1. Any person who, with a view to gain for themselves or another or with intent to cause harm to the data subject, causes harm to the data subject by acting in breach of Sections 123, 126 and 130 or else of the measures taken further to Section 129, shall be punished by imprisonment for between six months and one year unless the offence is more serious.
2. Any person who, with a view to gain for themselves or another or with intent to cause harm to the data subject, causes harm to the data subject by processing the personal data mentioned in Articles 9 and 10 of the Regulation in breach of the provisions set out in Sections 2-e and 2-g or the safeguards referred to in Section 2-f, or else by acting in breach of the measures adopted further to Section 2-p, shall be punished by imprisonment for one to three years unless the offence is more serious.
3. The penalty referred to in paragraph 2 shall also apply to any person who, with a view to gain for themselves or another or with intent to cause harm to the data subject, causes harm to the data subject by transferring the personal data to a third country or a international organisation in cases other than those permitted under Articles 45, 46 or 49 of the Regulation, unless the offence is more serious.
4. Where any of the offences mentioned in paragraphs 1 to 3 are reported to the public prosecutor, the latter shall inform the Garante thereof without delay.
5. The Garante shall transfer the records and findings gathered in the course of controls to the public prosecutor along with a reasoned report if there are grounds to believe that a criminal offence has been committed. Such records and findings shall be transferred to the public prosecutor no later than when the activities aimed at establishing the infringements of the provisions mentioned in this decree are concluded.
6. The penalty shall be reduced if the offender or the organisation has been the subject of an administrative fine imposed by the Garante in accordance with this Code or the Regulation on account of the same facts and such fine has been levied.

Section 167-a

(Unlawful communication and dissemination of personal data that are processed on a large scale)

1. Any person who, with a view to gain for themselves or another or with intent to cause harm, communicates or disseminates an automated filing system or a substantial part thereof containing personal data that are processed on a large scale, in breach of the provisions set

out in Sections 2-c, 2-f and 2-h, shall be punished by imprisonment for one to six years unless the offence is more serious.

2. Any person who, with a view to gain for themselves or another or with intent to cause harm, communicates or disseminates an automated filing system or a substantial part thereof containing personal data that are processed on a large scale shall be punished by imprisonment for one to six years if the data subject's consent is required with a view to any communication or dissemination and such consent has not been obtained, unless the offence is more serious.
3. Paragraphs 4 to 6 of Section 167 shall apply to the offences mentioned in paragraphs 1 and 2 hereof.

Section 167-b

(Fraudulent acquisition of personal data that are processed on a large scale)

1. Any person who, with a view to gain for themselves or another or with intent to cause harm, acquires, in a fraudulent manner, an automated filing system or a substantial part thereof containing personal data that are processed on a large scale shall be punished by imprisonment for one to four years, unless the offence is more serious.
2. Paragraphs 4 to 6 of Section 167 shall apply to the offence mentioned in paragraph 1 hereof.

Section 168

(Untrue Declarations to the Garante and Obstruction to the Discharge of Tasks or the Exercise of Powers by the Garante)

1. Whoever declares or certifies untrue information or circumstances, or else submits forged records or documents in the course of a proceeding or a fact-finding activity by the Garante shall be punished by imprisonment for between six months and three years, unless the offence is more serious.
2. Except for the cases under paragraph 1, whoever intentionally obstructs or disrupts a proceeding before the Garante or the fact-finding activities carried out by the Garante shall be punished by imprisonment for up to one year.

Section 169

(Security Measures)

(Repealed)

Section 170

(Failure to Comply with Provisions Issued by the Garante)

1. Whoever fails to comply with a measure adopted by the Garante pursuant to Article 58(2), letter f), of the Regulation, Section 2-g, paragraph 1, hereof and with the orders of general application mentioned in Section 21(1) of the legislative decree implementing Section 13 of Law No 163 of 25 October 2017 shall be punished by imprisonment for between three months and two years, where such measure is binding on them.

Section 171

(Violations of the provisions concerning remote surveillance and surveys of employees' opinions)

1. Any violation of the provisions referred to in Sections (4)1 and Section 8 of Law No 300 of 20 May 1970 shall be punished as provided for by Section 38 of that Law.

Section 172

(Additional Punishments)

1. Being convicted of any of the offences referred to in this Code shall entail publication of the relevant sentence pursuant to Section 36, paragraph 2 and 3, of the Criminal Code.

TITLE IV - AMENDMENTS, REPEALS, TRANSITIONAL AND FINAL PROVISIONS

CHAPTER I - AMENDMENTS

Section 173

(Convention Implementing the Schengen Agreement)

(Repealed)

Section 174

(Service of Process and Judicial Sales)

(Repealed)

Section 175

(Police)

1. (Repealed)

2. (Repealed)

3. For Section 10 of Law 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)

(Repealed)

Section 177

(Census Registers, Registers of Births, Deaths and Marriages, and Electoral Lists)

(Repealed)

Section 178

(Provisions Concerning the Health Care Sector)

(Repealed)

Section 179

(Other Amendments)

(Repealed)

CHAPTER II - TRANSITIONAL PROVISIONS

(Repealed)

Section 180

(Security Measures)

(Repealed)

Section 181

(Other Transitional Provisions)

(Repealed)

Section 182

(Bureau of the Garante)

(Repealed)

CHAPTER III - REPEALS

Section 183

(Repealed Provisions)

1. As of the date of entry into force of this Code, the following shall be repealed:

a) Law No 675 of 31 December 1996;

b) Law No 325 of 3 November 2000;

c) legislative decree No 123 of 9 May 1997;

d) legislative decree No 255 of 28 July 1997;

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 thereof;

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, Sections 12, 13, 14, 15, 16, 17, 18, 19 and 20 of Presidential Decree No 501 of 31 March 1998 shall be repealed.

3. As of the date of entry into force of this Code, the following 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 Law No 152 of 30 March 2001;

c) Section 4(3) of Law 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-c 1), second and third sentence, of decree-law No 70 of 28 March 2000 as converted, with amendments, into Law 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-a 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 Law 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, also by laws or regulations, shall be the one specified in said Code.

CHAPTER IV - FINAL PROVISIONS

Section 184

(Transposition of European Directives)

(Repealed)

Section 185

(Annexed Codes of Conducts and Professional Practice)

(Repealed)

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, ….