

FRA

Thematic Legal Study on assessment of
data protection measures and relevant
institutions
[Italy]

Authors:
Marta Cartabia
Giulia Tiberi
Giulio Enea Vigevani

[Italy]
February 2009

DISCLAIMER: This thematic legal study was commissioned as background material for the comparative report on *Data protection in the European Union: the role of National Data Protection Authorities* by the European Union Agency for Fundamental Rights (FRA). It was prepared under contract by the FRA's research network FRALEX. The views expressed in this thematic legal study do not necessarily reflect the views or the official position of the FRA. This study is made publicly available for information purposes only and do not constitute legal advice or legal opinion.

Contents

Executive summary	4
Executive summary	4
1. Overview.....	7
1.1. Constitutional standards	7
1.2. International standards.....	8
1.3. European Union standards.....	9
1.4. Data protection legislation.....	10
2. Data Protection Authority	13
2.1. Structure and organization.....	13
2.2. Powers and functions.....	14
2.3. Compliance with the EU legal framework	14
2.4. The remit of the data protection authority	15
2.5. Human and financial resources.....	16
2.6. Independence and autonomy	16
2.7. Investigative powers	17
2.8. Monitoring powers	17
2.9. Publicity of decisions and/or opinions.....	18
2.10. Relevance of the Opinions of Article 29 Working Party	19
2.11. Advisory powers.....	19
2.12. Awareness raising role	20
3. Compliance.....	21
3.1. Duties of registration and duties of approval of sensitive data	21
3.2. Appointment of staff in charge of the processing	22
4. Sanctions, Compensation and Legal Consequences	23
4.1. Remedies: the alternative jurisdiction of the DPA and the courts	23
4.1.1. Administrative remedies	23
4.1.2. Non-Judicial Remedies	23
4.1.3. Judicial Remedies	24
4.2. Compensation payments and sanctions	25
4.3. Follow-up of the <i>ex officio</i> surveys	26
4.4. Effectiveness of personal initiatives of data subjects	27
4.5. Workers' data protection	29
5. Rights Awareness.....	32
6. Analysis of deficiencies.....	33
6.1. Deficiencies	33
6.2. Exemptions	33
6.3. Required interventions.....	34
7. Good practices	36

8. Miscellaneous	39
Annexes	40

Executive summary

- [1]. The Italian legal system provides a high level of protection of Data Protection Rights. Although the Italian Constitution does not encompass an explicit provision dedicated to data protection, since the 70s a right to privacy has been worked out by the Italian *Corte costituzionale* [Constitutional Court] by means of interpretation of several articles of the Constitution. Moreover, Italy complies with its international obligations and has fully implemented all the relevant European Community directives. Special attention is paid by the constitutional and ordinary judges to the ECHR, the decisions of the ECtHR and the EU Charter of fundamental rights.
- [2]. A specific Data Protection Legislation was firstly issued in 1996, in order to implement the European Union Data Protection Directive of 1995. Before then, the Italian legal system offered protection to privacy and personal data rights only in specific sectors, such as in working places (Italy/law n. 300/1970). An important revision of the data protection legislation took place in 2003, when the Data Protection Code entered into force. At present the Code provides for a comprehensive regulation of data protection. The Code has taken important steps towards simplification of all procedures connected with all processing operations of personal data , without prejudice for a high standard of guarantee for the data subject. The Italian Data Protection Code is enforced by the *Garante per la Protezione dei Dati Personali* [DPA].
- [3]. The “Garante” (DPA) is the Italian independent administrative authority entrusted with the duty to protect fundamental rights with regard to the processing of personal data. It is a collegiate body composed by four members, elected by the Parliament. Its autonomy from political and economical powers is granted overall by its long-term office, the cases of incompatibility between the office of member of the Garante and other public and private offices and the prohibition of re-election of its members.
- [4]. The Code provides that the DPA has a significant number of heterogeneous functions. On the whole, the powers given to the DPA seem wider than the requirements of Article 28 of Directive 95/46/EC and could be regarded as sufficient to achieve effective data protection. In fact, the DPA has played a remarkable role in the protection of privacy rights. It is worth noticing the use of its investigative and monitoring powers, by which the DPA is developing new methods and strategies to prevent violations, to identify the priorities of intervention and to improve its role of policy making in this sector. Critical situations are related to the advisory role of the DPA for the political institutions: whereas the law requires the Government to consult with the DPA when drafting regulations and administrative instruments that are liable to have an impact on personal data protection, in a high number of important cases the DPA has not been consulted. It is also worth noticing the contribution of the

Italian DPA to the activities of the Art. 29 Working Party and to other international and European bodies and networks.

- [5]. With regard to the duties of registration and requesting approval of sensitive data, there is a tendency to simplification and reduction of the cases of registrations and an increase in the use of general authorisations to homogeneous categories of sensitive data processing
- [6]. Processing operations may only be performed by persons that act under the direct authority of either the data controller or the data processor by complying with the instructions received. They must be nominated in writing by specifically referring to the scope of the processing operations that are permitted and must receive adequate training.
- [7]. The Data Protection Code has strengthened the individuals' data protection rights, allowing them to exercise their rights and instigate proceedings more easily. The Code provides several remedies, both administrative, non-judicial and judicial. Data subjects can settle disputes, alternatively, either through the courts or by lodging a complaint with the DPA. The complaint before the DPA is an alternative approach to legal action in courts and allows data subjects to obtain expeditious decisions.
- [8]. Failure to comply with the provisions of the Code involves the application of compensation payments, administrative sanctions and criminal sanctions. Inversion of the burden of proof is provided, exempting the data subject claiming a right from having to prove the facts on which it is founded and it then lies with the alleged defaulter, the person processing the data, to prove that damage did not occur.
- [9]. Infringements of personal data protection provisions have been increasingly identified, in recent years, by the Data Protection Authority through its own motion investigations, rather than following claims or complaints. Investigations have turned out to be, in many cases, more effective than the complaints lodged by individual citizens as they focused on a growing number of issues broader in scope, as well as on major areas of societal life and the activities of both public and private databases. Moreover they have a preventive effect on violations of Data Protection rights.
- [10]. High level standards of data protection and privacy are provided for workers. Processing of data must comply with data protection safeguards and in pursuance of the binding principles of necessity, data minimization and fairness.
- [11]. The Italian data protection legislation has a wide scope of application and provides for high level standards of protection. Still, some deficiencies might be envisaged concerning safeguards for databases; in the relationship between media, journalism and personal data protection; in the processing of personal data by judicial authorities, with a special concern for the disclosure of

telephone wiretapping activities. Deficiencies could be reduced or mitigated with an appropriate resource allocation in order to meet the technical standards and security measures of protection required. Amendments to legislation could be necessary, in some cases, especially in order to boost the supervisory and control functions of the DPA, with special reference to inspection and sanctioning or injunction powers.

- [12]. The dynamic and proactive stance of the Italian Data Protection Authority has played a major role in providing effective data protection, also due to the development of innovative working methods. In the Italian approach, good practice for effective data protection is to be considered: the prior checking of the compliance with standards and provisions provided by data protection regulation; the adoption of guidelines, in order to facilitate compliance; a flexible type of self-regulation, based on codes of practice, together with a simpler and more effective data protection for workers and businesses.

1. Overview

1.1. Constitutional standards

- [13]. The Italian Constitution, adopted in 1948, does not encompass specific provisions protecting privacy and confidentiality and the protection of personal data. Nevertheless, a right to confidentiality has been recognised at constitutional level by the *Corte costituzionale* [Constitutional Court] as a “penumbra” of various expressed provisions contained in the Italian Constitution, together with other provisions set forth by international conventions, and specifically Article 8 of the European Convention on Human Rights (hereinafter ECHR) ratified by Italy with Law n. 848/1955,¹ which enumerates explicitly the right to respect for private and family life as a fundamental human right (see below for the status of ECHR in the Italian legal system). The overwhelming majority of scholars and judicial decisions relied on Article 2 of the Italian Constitution as the foundation of privacy, regarded as an inviolable right.
- [14]. Several limited provisions relating to privacy were considered as well a source for an unexpressed right to privacy and confidentiality: Article 13 on personal freedom, Article 14 on domicile and Article 15 on secrecy of correspondence. Thus, since 1973 the Constitutional Court has specified that the protection of privacy is a fundamental right of the citizen, protected under Article 2 of the Constitution² and the *Corte di Cassazione* [Italian Supreme Court] recognised a right to protection of private life and confidentiality based on the constitutional provisions,³ protecting human dignity, personal liberty, personal domicile, and confidentiality of correspondence. In 2002, the Constitutional Court in a case dealing with violations of domicile, restated the protection of privacy at constitutional level and cited, along with the above mentioned constitutional provisions, the ECHR and the European Charter of fundamental rights as sources of this right (see below, section 1.2). Effective Protection of confidentiality has also been required by the Constitutional Court for medical treatments: in decision n. 218/1994, regarding AIDS, the Court stated that “Any investigations including samples and analyses, as well as being medical treatments, require effective safeguards for confidentiality – also in order to prevent an individual from being discriminated against in his/her occupational and social life”.

¹ Italy/legge n. 848/1955 (04.08.1995) available at <http://www.privacy.it/legge1955848.html> (07.01.2009).

² Italy/Corte costituzionale n. 38/1973 (05.04.1973).

³ Italy/Corte di Cassazione n. 2129/1975 (27.05.1975).

- [15]. It is also important to stress that the law-making power on personal data protection is exclusively entrusted to the State and cannot be granted to the autonomous regions.⁴

1.2. International standards

- [16]. Italy is a member of several organizations that influence the country's treatment of privacy and personal data. In particular, Italy has ratified and implemented the relevant international instruments⁵.
- [17]. It is worth stressing a recent development in the Italian system concerning the legal value of the ECHR. In its decisions n. 348-349/2007⁶ the Italian Constitutional Court affirmed that the ECHR and the decisions of the European Court of Human Rights (hereinafter ECtHR) will be used in the judicial review of legislation by the Constitutional Court itself, in order to ensure that Italian legislation will always comply with the aforementioned ECHR and the interpretation of it given by the ECtHR. The Italian Constitutional Court pays great attention towards the Strasbourg Court's case law. In the above mentioned decisions, as well as in many others taken in recent years, the Constitutional Court regularly refers to the norms of the European Convention "as interpreted by the European Court of Human Rights".⁷
- [18]. At the international level, considerable importance should be attached to the work of the Garante, which contributed first and foremost to the activities of the Article 29 Working Party, composed of representatives from the EU's data

⁴ In an important decision adopted following a complaint lodged from the State against some articles of a regional law, the Constitutional Court ruled that the said provisions were in breach of constitutional principles on the division of competence between Law and State. The Court ruled that the measures in question had an impact on the right to personal data protection and for this reason fell within the scope of the competences entrusted to the State by Article 117 of Italy's Constitutional Charter. Italy/Corte costituzionale n. 271/2005, (23.06.2005)

⁵ Council of Europe instruments: a) Article 8 of the European Convention on Human Rights (ECHR), including the case law of the European Court on Human Rights, on the protection of privacy and private life; b) Basic Principles contained in the Appendix to the Recommendation Rec(87)15 adopted by the Committee of Ministers on 17 September 1987, at 401st meeting of the Ministers' Deputies; c) The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981); d) The Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding Supervisory Authorities and Transborder Dataflow (2001). The Convention on Human Rights and Biomedicine (1997). UN instruments: Article 17 of the International Covenant on Civil and Political Rights (ICCPR, 1966) and the General Comment No. 16 on Article 17 ICCPR; The Guidelines for the Regulation of Computerized Personal Data Files adopted by a resolution of the General Assembly of the United Nations on the 14th December 1990.

⁶ Italy/Corte costituzionale n. 348-349/2007 (22.10.2007).

⁷ Italy/Corte costituzionale n. 348/ 2007, par. 4.6.

protection authorities,⁸ by working out opinions on geolocalisation, intellectual property, use of RFID devices, e-health, exchange of data for judicial co-operation and security purposes, in view to the creation of a new information system (SIS-II). The same importance must be attached to the work done by the Garante within the framework of the Schengen, Europol, and Eurodac Joint Supervisory Authorities, the Chair of the Working Party on Police and Justice, the Council of Europe, and the OECD working party in charge of privacy issues. The Garante hosted also the Annual Conference of European Data Protection Authorities, that took place in Rome in April 2008.⁹ Moreover it is worth recalling that Italy is a member of the Organization for Economic Cooperation and Development (OECD) and has adopted the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

1.3. European Union standards

- [19]. As regards EC law, Italy complies with the requirements of Council Directive 95/46/CE (24.10.1995) and Council Directive 2002/58/CE (12.07.2002). It is here worth remarking the significance attached by the Italian Constitutional Court and other lower judges to the EU Charter of Fundamental Rights. In decision n.135/2002, the Constitutional Court¹⁰ has directly referred to the European Charter of Fundamental Rights. In a case dealing with videotapes the Court stated that “a restriction in the typology of interferences of public authority in the liberty of domicile would not be compatible with (...) the Charter of the Fundamental Rights of the European Union proclaimed in Nice in December 2000 (artt. 7 and 52)”. The Court clarified that a reference was made to the Charter “notwithstanding devoid of juridical value, because of its character which is expressive of the common principles of European legal systems”. The fact that the Italian Court mentioned the Charter (and other international agreements) as an argument *ad adiuvandum*, in support of its motivations, when on the contrary such a reference was redundant for the decision in the specific case, is particularly interesting because it seems that the Court wanted to make a point of taking into consideration the European Charter. With its statement the Court attached a value to the Charter regardless of its nature and legal status.

⁸ See Art.29 Data Protection Working Party

http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm (10.01.2009)

⁹ The 2008 Annual Conference of European Data Protection Authorities had as a motto “What Outlook for Privacy in Europe and Beyond”, see <http://www.springconference2008.it> (10.01.2009)

¹⁰ Italy/Corte costituzionale n. 135/2002 (24.04.2002).

1.4. Data protection legislation

- [20]. The Italian Data Protection Act was enacted in 1996 (Italy/legge n. 675/1996). The Act was intended to fully implement both the European Union Data Protection Directive¹¹ at national level and introduce the necessary provisions to implement Convention n.108 of the Council of Europe. The instruments for ratification of this latter Convention were introduced on 29 March 1997 and the Convention entered into force in Italy on 1 July of the same year.
- [21]. Transposition was ultimately finalised in 2003 by the Personal Data Protection Code,¹² which entered into force on 1 January 2004. The new Personal Data Protection Code consolidates all the legal provisions so far regulating personal data protection in Italy, thus considerably simplifying and harmonising the legal framework. In fact, the Code replaced the former Data Protection Act and the various decrees enacted after 1996 to regulate data protection in specific sectors, such as security requirements, the processing of medical information, the processing of information for journalistic, scientific or research purposes, and personal data held by public bodies.¹³ The new Data Protection Code (hereinafter, the Code) therefore is a comprehensive regulation on the matter.¹⁴ Furthermore, the Code has upgraded the previous regulations into primary legislation, thereby affording a high level of protection to the rights and freedoms concerned. Simplification, harmonisation and effectiveness are the underlying principles of the Code with regard to exercise of data subjects' rights and the fulfilment of the relevant obligations by data controllers.
- [22]. The Code is divided in three parts: the first contains provisions dealing with the rules applicable to the processing of personal data in the public and private sector; the second deals with "special requirements," which would apply in specific sectors, such as debtors or the health sector; and the third concerns the available remedies and lists the sanctions provided for in case of non-compliance (administrative and judicial issues). The Code strengthens the protection for data subjects while simplifying the applicable rules. In

¹¹ Council Directive 95/46/EC (24.10.1995)

¹² Italy/Decreto legislativo n. 196/2003 (30.06.2003) available at <http://www.parlamento.it/leggi/deleghe/03196dl.htm> (07.01.2009)

¹³ See, respectively, Italy/ Decreto del Presidente della Repubblica n. 318/1999 (28.07.1999); Italy/ Decreto legislativo n. 282/1999 (28.07.1999); Italy/Decreto legislative n. 171/1998 (13.05.1998); Italy/Decreto legislative n. 281/1999 (30.07.1999); Italy/ Decreto legislativo n. 135/1999 (11.05.1999).

¹⁴ The new Code on Personal Data Protection also implemented Council Directive 2002/58/EC (12.07.2002), which replaced Directive 97/66/EC on data protection in the telecommunications sector; the latter directive had been transposed into Italy's national law by means of Italy/Decreto legislativo n.171/1998 as amended by Italy/Decreto legislativo n. 467/2001 (28.12.2001). Title X, articles 121 to 133, of the Code specifically address electronic communications by transposing the new EC directive, in particular as regard the opt-in — i.e. prior consent — principle for the inclusion of a data subject's data into directories of subscribers to electronic communications services (Article 12) as well as sending unsolicited commercial communications (Article 13).

comparison with the EC Directive and the European Convention, the scope of application of the Italian legislation is wider in that it covers any manual or automated processing, by any entity established in Italy, of data of a physical person or legal entities undertaken by both government agencies and the private sector. As the previous law, also the Code conforms to the following principles: a) complete information to the data subject on rights granted by the law; b) previous consent of the data subject for all kind of data processing; c) fairness and lawfulness of the processing of data by the data processor.

[23]. Moreover the Code provides the new following principles:

- *Notification*: One of the key targets of simplification was the notification process: the Code reduced the scope of the requirements to be met by both private entities and the public administration. The new system is in line with the EU law which allows the notification process to be simplified in cases where data processing does not adversely affect the rights and freedoms of data subjects (Article 18, paragraph 2 of the Council Directive 95/46/CE (24.10.1995). Under the Italian Code, organisations are only required to notify the DPA when processing higher-risk categories of data. These include genetic and biometric data, data processed for the purpose of analysing or profiling individuals, and credit-related information (Article 37 of the Data Protection Code). This approach aims at making the process more transparent and understandable for individuals.
- *Data minimization*: Article 3 of the Code introduces the element of data minimisation into Italian data protection, providing that the information systems and software shall be configured by minimising the use of personal data and identification data: the Code thus encourages organisations to make use of non-personal data whenever possible.
- *Data subject rights*: The Code aims at strengthening individuals' data protection rights and makes easier the access to remedies and more effective the procedures before the DPA and the judicial authorities (see below, section 4.1).
- *International data transfer*: In line with the directive, the mechanism applying to transborder data flows was also simplified. The new Code has incorporated and, to some extent, updated the previous rules on data transfers (Articles 42-45 of the Code). Whereas previously businesses had to notify the Garante of their intention to transfer data outside the EU, under the new system companies will only have to provide notification in cases in which the transfer of data could prejudice data subjects' rights. In this way, data controllers are no longer required to await expiry of the term previously provided for by the law in order to perform the transfers. The rules for legitimising transfers to non-EU countries can be found in Article 43 of the Code and include consent, meeting contractual obligations, public interest requirements, safeguarding life/health, investigations by defence counsel, use of publicly available data, processing for statistical/historical purposes.

Additional provisions for legitimising transfers are laid out in Article 44 of the Code and include transfers to countries that are deemed to provide adequate protection according to the European Commission, or the adoption of contractual safeguards.

- [24]. The Italian legal system thus provides a high level of protection of Data Protection Rights. A few deficiencies in effective data protection have been identified in the Italian debate in the following areas: a) relationships between media and data protection (especially in case of dissemination by the media of data originally collected for judicial purposes through the publication of wiretapping contents); b) safeguards for public databases (especially for police databases and those serving national and State interests), which need to be listed in order to accomplish how many large-sized public databases are in existence and what types of database are available; c) level of data protection assured by judicial and legal practitioners in courts and in the business sector; d) powers of the DPA (especially inspection and sanctioning/injunction powers, which need to be boosted).

2. Data Protection Authority

2.1. Structure and organization

- [25]. The Italian *Garante per la protezione dei dati personali* [Data protection authority] is a supervisory authority entrusted with the purpose to protect fundamental rights with regard to the processing of personal data. It was instituted by Law 675/1996,¹⁵ implementing Council Directive 95/46/CE (24.10.1995). A relevant legislative reform occurred in 2003, when the Government passed the Data protection Code with the decreto legislativo [legislative decree] n.196/2003.¹⁶ The Code codifies the entire previous legal framework.¹⁷ According to article 153(1) of the Code, the Garante shall act fully autonomously and independently in its decisions and assessments.
- [26]. According to article 153(2) of the Code, the Italian data protection authority shall be a collegiate body composed of four members, two of whom shall be elected by the Chamber of Deputies and two by the Senate through a specific voting procedure. The voting system provides for an equal representation of majority and minorities. The members shall be experts in the field of law or computer science and shall ensure independence. The President and the Vice-President are elected by the members themselves. After an amendment approved in 2008, the appointment in office is seven years, not renewable. The law provides also for an incompatibility clause that forbids the members of the Garante to carry out professional or advisory activities, manage or be employed by public or private entities or hold elective offices. The staff, the organisation, and the budget of the Office of the Garante are regulated by article 156 of the Code. It provides that the office shall be under the authority of a secretary general. The permanent staff cannot exceed the number of one hundred twenty five employees; at the end of 2008 the total staff was composed by 97 people. Where necessary, the Garante may be assisted by consultants or employees, employed with fixed-term contracts. With regard to the organisation, the Garante sets out, by regulations that are published in the Official Journal, the organisation and operation of its Office, career patterns and recruitment, allocation of staff, staff regulations and salaries, administration and accounting mechanisms. The operating costs concerning the Garante are covered by a fund set up for this purpose in the State budget.

¹⁵ Italy/legge n.675/1996 (31.12.1996)

¹⁶ Italy/Decreto legislativo n. 196/2003 (30.06.2003)

¹⁷ The Code is available also in English at:

<http://www.garanteprivacy.it/garante/navig/jsp/index.jsp?folderpath=Normativa%2FItaliana%2FIIL+Codice+in+materia+di+protezione+dei+dati+personali> (07.01.2009).

2.2. Powers and functions

- [27]. The powers and functions of the Garante are listed in article 154 of the Code. This list is heterogeneous and not complete and it is necessary to take into account also the other specific functions included in other provisions of the Code. These functions could be classified in five categories: supervisory and control, decision-making, quasi-legislative, advisory, and quasi-judicial powers. The tasks to be discharged by the Garante are listed in detail in art. 154 (1) of the Code.
- [28]. The Garante has also supervisory or assistance tasks concerning personal data processing provided for by international agreements or by EC regulations. In other provisions of the Code are listed other functions, by which the Garante participates in the definition of the legal framework of the data protection. The measures that shall be adopted are defined as: individual authorisations (permissions issued by the Garante to the data processors before the sensitive data processing), general authorisations (authorisations issued by the Garante, applying to specific categories of data controller or processing), measures and precautions (rules laid down by the Garante to safeguard data subjects in processing operations carrying specific risks)

2.3. Compliance with the EU legal framework

- [29]. The powers given to the Italian supervisory Authority meet the requirements of Article 28 of Council Directive 95/46/EC (24.10.1995). Note the particular structure and richness of judicial and non judicial remedies offered by the Italian Law (see below section 4.1)
- [30]. The Garante gives opinions whenever required.¹⁸ Article 154(4) provides also that the Garante shall be consulted by the executive power in the preparation of regulations that have effects on privacy. Regarding its investigative powers, Italian law provides inter alia that the Garante may request the data controller, the data processor, the data subject or a third party to provide information and produce documents (article 157) and may order that data banks and filing systems be accessed and audits on the spot be performed (article 158). The law lays down wide and effective powers of intervention: the Garante may order, also ex officio, that the data controllers take such measures as necessary to bring the processing into line with the provisions in force and may block or prohibit the processing, in whole or in part.

¹⁸ As a general rule, the Garante's opinion shall be rendered in the cases at stake within forty-five days of receiving the relevant request. Upon expiry of said term, the requesting administrative agency may proceed irrespective of the acquisition of the Garante's opinion [article 154(5)].

- [31]. Regarding the powers of the Garante related to the cases where the data subject's rights have been violated, the Italian legislator did more than giving to the authority the power to engage in legal proceedings and bring violations to the attention of judicial authorities. As a matter of fact, the legislator has extended the power of the authority which has the function to decide directly the complaints lodged concerning the protection of the rights foreseen at article 7 of the code (article 145). This complaint to the Garante is expressly qualified by the law as an alternative to the judicial action. The competence over the disputes related to provisions issued by the Garante, shall lie with judicial authorities.
- [32]. In short, the Italian Garante is not only a supervisory authority, but it is also a guarantee authority, specialised in the protection of fundamental rights and entrusted with powers similar to those of the judicial authority. The powers given to the data protection authority guarantee the achievement of the purposes of personal data protection required by the Community legislation. What seems to be necessary, then, are not new powers and functions, but rather a major and more punctually effective involvement of the Garante by the Government, more certainty about the budget and the staff, and above all the enhancing of the sanctioning power through the introduction of more substantial penalties having a stronger deterrent power. In fact, sometimes, the obligation of the Government to consult the Garante when drawing up regulations liable to produce effects on data protection is not fulfilled; this is not a systematic practice, but it is a point of concern underlined in many Annual Reports (see para. 2.11). As for the sanctioning power, the administrative sanctions vary from € 3.000 to € 60.000 and this can decrease the actual level of compliance (see para. 4.2, footnote 37).

2.4. The remit of the data protection authority

- [33]. The Italian law provides the Garante with functions belonging to different areas: normative, regulatory, administrative and quasi-judicial. The Garante is independent with regard to other powers. Its functions are strictly connected with its main task which is the protection of the fundamental rights of the person. Article 2 of the Code establishes as fundamental remit of the data protection authority the task to ensure "that personal data are processed by respecting data subjects' rights, fundamental freedoms and dignity, particularly with regard to confidentiality, personal identity and the right to personal data protection".
- [34]. In this framework, the Garante represents an Authority with powers and limits which are not precisely defined, having the opportunity to intervene in almost any case in which the rights it has the task to protect are violated.. The Garante mandate is related to all social economical and cultural aspects where personal data protection is required. The most important protected sectors are the public

administration activities, health, work, credit sector, insurance, journalism, communications, video surveillance, marketing. For this reason the majority of Garante's deliberations deal with these aspects.

2.5. Human and financial resources

- [35]. The Garante, compared to other similar bodies, has at its disposal a quite limited staff, not proportionate with the number and the complexity of the functions that the authority itself is called to carry out. On December 31 2007, the Office was composed, by 87 people. Besides, the Authority employs 13 units under contract, some of them only for short period of time. The budget is also limited; in 2007 the total revenue amounted to about 20.7 millions of Euros. The contribution of the State, equal to 18.7 millions, is decreased of about 1 million Euros compared to 2006.¹⁹ The reduction of the budget and the fact that the number of employees is lower than the staff provided for by the law raise a serious question related to the possibility of the DPA to carry out its demanding duties effectively. Nonetheless, there can be observed a positive inversion of tendency. In 2007, the Authority was increased by 25 units, from 100 to 125, in order to discharge its institutional tasks better with particular regard to its supervisory and control functions.

2.6. Independence and autonomy

- [36]. The Italian law establishes that the members of the DPA should be elected from the assemblies of the two Chambers, which is similar compared to the appointment of one third of the members of the Constitutional Court. This choice underlines the legislator's concern for the independency of the Garante. The voting system is the known as "limited vote"; thus, it is impossible that all the members of the Garante belong to the political majority. The law does not provide for strict requirements of eligibility. It simply establishes that members shall be persons with proven experience in the field of law or computer science and that experts from both sectors shall have to be included. The political autonomy is also guaranteed by the strict incompatibilities foreseen by the Italian law, by the long term appointment, two years longer than the term of the Chambers, and by the prohibition of recall and re-election. The independency is also reinforced by a large autonomy in its own organization, which concerns among others, the staff, the management, the organization and the functioning of the office and the management of the expenses.
- [37]. Therefore, there are no serious concerns about the independency rules. The members of the authority demonstrated to be skilled and independent from the

¹⁹ See 2007 Annual report, pg. 211 available at:
<http://www.garanteprivacy.it/garante/doc.jsp?ID=1533131> (05.01.2009).

political and economic power. Possible concerns could arise if, in future appointments, the political affiliation criteria prevail on the requirement of competence and effective expertise of DPA members.

2.7. Investigative powers

- [38]. Regarding the investigative powers, Italian law provides *inter alia* that the Garante may request the data controller, the data processor, the data subject or a third party to provide information and produce documents (article 157 of the Code) and may order that data banks and filing systems be accessed and audits on the spot be performed (article 158). The law provides that the addressee of the request is obliged to answer.²⁰
- [39]. The Garante is developing strategies to improve preliminary investigations aimed at preventing violations, also when there are no direct reports by victims. The plan is focused on increasing the number of inspections, on introducing the institution of inspector team with specific abilities, and on checking of homogeneous categories of data processors Pursuant to this new strategy the voluntary inspections in 2007 amounted to 452 (compared with 40 in 2002, 230 in 2005 and 250 in 2006).²¹ Eighty per cent of this activity is activated *ex officio*; the remaining part comes from citizens' claims, reports and complaints. The fact that in the last years the Garante has developed such a proactive role is explained by the adoption of new control methods. Pursuant to the Regulation n. 1/2007,²² the Garante establishes, every six months, the guidelines of the inspective activity of its Office, determining the areas which should be supervised and the goals to achieve. This approach allows, thanks also to inspections on subjects acting in the same field, to examine compliance with the law. The main areas involved in these programs are: telephone operators about call center and *traffic* data, pharmaceuticals industry, banks, with reference to e-banking services.

2.8. Monitoring powers

- [40]. The monitoring tasks are provided by article 154 (1) a) and b) of the Code and specified in other provisions within the Code itself (as for example, article 8, article 37). The Data Protection Authority uses two different ways to monitor whether the processing is in compliance with the rules and in observance of the notification and whether there exist violations of personal data. The first one consists on claims, reports and complaints received from victims of alleged

²⁰ According to article 164 of the Code, "whoever fails to provide the information or produce the documents requested by the Garante ... shall be punished by a fine ...".

²¹ See 2007 Annual report, pg. 151.

²² Available at <http://www.garanteprivacy.it> [doc. web n. 1477480] (10.01.2009).

violations (article 141 and ss. of the Code). The access to the Garante generally does not require formal procedures.²³ The second way is based on “the facts and or circumstances to be prosecuted ex officio which the Garante knows either in discharging or on account of its duties” [article 154(1)]. Thanks to the processing operations registry, which contains all the notifications that the data controller is bound to refer to, the Garante has the opportunity to check the correct use of data, then to prosecute ex officio illegal situations. The Garante, informed of a violation, conducts preliminary investigations in order to verify the complaints and to decide on the measures to be taken.

- [41]. In 2007, the overall number of complaints fell from 435 in 2006 to 316, which proves possibly that there is an increased compliance with the law. The remarkable increase in the replies to claims and reports – from 2717 in 2006 to 3078 in 2007 – proves the growing number of issues that are broader in scope whilst advisory and guidance activities have also risen.²⁴ An important step is the approval in 2007 of the Regulation n. 1/2007,²⁵ in order to specify the criteria for the examination of claims and reports, in respect with the budget of the Garante (seriousness of the violation and the damages, probability of the existence and effects of the violation). On the basis of such criteria, the Garante set every six months the time-frame of the job of the collegiate and its priorities in the examination of the claims and reports. The aim is to improve the monitoring functions not only as an instrument of repression of the violation, but also as an instrument of policymaking.

2.9. Publicity of decisions and/or opinions

- [42]. The decisions and the opinions of the data protection authority are available to the public in a number of ways. The main decisions and the documents, are published online²⁶ in a monthly bulletin, where it is also possible to find the answers to incoming questions which are of general interest. Every year the Garante publishes an annual Report,²⁷ to provide an overview of its work. In this document, the Authority summarizes and presents in a systematic way the activity developed during the year. The Report is presented to Parliament with a speech delivered by the President of the DPA. The speeches are available also

²³ The official web site of the Garante dedicates for this purpose a special s, “Contatta il Garante” [Contact the Garante] with all the instructions to reach it. Reports could simply be sent by mail or e-mail. For claims and complaints it is requested to call the public relations officer in order to obtain all the relevant information and the format to fill in (see part. 4).

²⁴ Data from 2007 Annual report, pg. 197 ss.

²⁵ <http://www.garanteprivacy.it> [doc. web n. 1477480] (10.01.2009).

²⁶ <http://www.garanteprivacy.it/garante/navig/jsp/index.jsp?folderpath=Provvedimenti> (08.01.2009).

²⁷ Available at

<http://www.garanteprivacy.it/garante/navig/jsp/index.jsp?folderpath=Attivit%E0+dell%27Autorit%E0%2FRelazioni+annuali+al+Parlamento> (08.01.2009).

in English in the DPA's website. Furthermore, the Italian Authority issues several press releases and publishes every week an online Newsletter.²⁸

2.10. Relevance of the Opinions of Article 29 Working Party

- [43]. The opinions of the Working Party established under Article 29 of Council Directive 95/46/EC (24.10.2995) are on the whole considered as an important source of inspiration for the Garante. Many of its decisions refer directly to the Working Party's opinions. These opinions have influenced significantly the Authority's choices. For example, the guidelines on the processing of data by private employers, issued in 2006,²⁹ are based on the Opinion 8/2001, concerning the processing of personal data in the employment context, issued September 13, 2001 by the Working Party. We can find other references to the opinions of the Working Party in a number of important decisions.³⁰ Frequently, the decisions of the Garante contain the statement that they are in line with the opinions of the Working Party.
- [44]. More generally, the Italian DPA has historically been one of the most active bodies in cooperating with the European authorities working on the protection of personal data. In the scenario of a more strict collaboration, the Garante has frequently suggested to provide the Working Party on Police and Justice (WWPJ), mandated by the European data protection authorities to monitor data protection developments as related to judicial and police co-operation, with both a clearer regulatory framework and new competences.

2.11. Advisory powers

- [45]. Among the main tasks of the Data Protection Authority the advisory one is very important. It links the tasks performed by the Garante to the political institutions. Under article 154(1) of the Code, the Garante has to draw the attention of Parliament and Government to the advisability of legislation as required by the need to protect the rights, fundamental freedom and dignity, also in the light of sector developments. Under article 154(4) of the Code, the Prime Minister and each Minister are required to consult the Garante when

²⁸ Available at <http://www.garanteprivacy.it/garante/navig/jsp/index.jsp?folderpath=Newsletter> (10.01.2009).

²⁹ <http://www.garanteprivacy.it> [doc. web n. 1364099] (10.01.2009).

³⁰ Among many others, in 2005 about processing of children data, fingerprints detection in the workplace, radio frequency identification-Rfid; in 2006 about biometric data, smart-cards in the public transportations, transfer of personal data abroad; in 2007 about the processing of data detected on the Internet and e-mail in the workplace, traffic data conservation, processing of genetic data.

drafting regulations and administrative instruments that are likely to have an impact on personal data protection. The Garante gives also opinions whenever required.

- [46]. As far as parliamentary hearings are concerned, the Garante was heard several times by Parliament during the last years, with regard to major issues debated by the competent parliamentary committees (concerning e.g. technological innovations in the public administration, the so-called biological will, the Schengen database, consumer fraud, the Register of Tax Registers). For what concerns the opinions ex article 154(4), in 2007 the Garante rendered 16 opinions to the Government, 8 of which concerned databases and the computerisation of public administrative bodies (the opinions were 13 in 2005, 27 in 2001, 70 in 2000). Nevertheless, from many years the Garante highlighted a number of cases where the Authority has not been consulted, even though some of them could be considered as significant measures.³¹ The lack of an prior opinion issued by the Garante when required by the law represents both a violation of the EC obligations and a possible underestimation of the aspects concerning the protection of the privacy in important political choices.

2.12. Awareness raising role

- [47]. During the last years, the Garante attempted to intensify the awareness of the citizens and companies of the importance of the protection of personal data. The presence in the media of topics concerning personal data protection and, in particular, the activity of the Garante itself, has demonstrated a progress. Furthermore, the organization every year on the Data Protection Day aims at creating a communication channel with the young generations. All this is intended to provide the citizens with a stronger acknowledgement of their rights. For example, claims in accordance with article 7 of the Code are more and more known; and even though the number of the actions is decreased in comparison with the uncontrolled proliferation of the last years but they are written in a more correct way.

³¹ See 2007 Annual report, pg. 18-19, and 2006 Annual report, pg. 14, where the Garante underlines that the DPA has not been consulted during the approval of some procedural regulations on relevant matters, such as: land register, traceability of payments, and bank accounts, passports, registration through ICT tools of judicial acts.

3. Compliance

3.1. Duties of registration and duties of approval of sensitive data

- [48]. After the entry in force of the new Code in 2003, the duties of registration of data processing operations have been simplified. Pursuant to article 37(1) of the Code, a data controller has to notify the processing of personal data he/she intends to perform if the said processing concerns the activities specifically indicated by the Code.³² Moreover, article 37(2) gives to the DPA the discretionary power to modify the lists, adding processing operations not included, that are liable to be prejudicial to rights and freedoms, and providing an exemption for others.³³ The Garante enters the notifications submitted into a publicly available register of processing operations, that may be accessed freely online. The notification procedure is made through the DPA's website and is simple and efficient. The Garante made significant steps to reduce the information required, to simplify the procedure, and to make public the register. According to the official reports of the DPA, the number of data protection registrations drastically decreased from 17.500 in 2001 to 978 in 2007.³⁴
- [49]. Regarding the request for approval for the processing of sensitive data, article 26 of the Code provides the principle that sensitive data may only be processed after the data subject's written consent and the Garante's prior authorisation. The Garante's decision concerning the request for authorisation is communicated within forty-five days and may establish measures and precautions in order to safeguard the data subject. There are cases where sensitive data may be processed without consent, subject to the Garante's authorisation: e.g. when the processing is carried out to comply with obligations and/or tasks laid down by laws, regulations or Community legislation. The Garante, when the processing is compulsory by law, issues general authorisations to homogeneous categories of data controllers or processors (e.g. employers, professional men). These authorisations provide for uniform rules and aim to eliminate the request of authorisations by each data controller.

³² Among them, genetic and biometric data; data disclosing health, sex life and the psychological sphere; data aimed at profiling the data subject and/or the personality; sensitive data stored in data banks for personnel selection purposes on behalf of third parties, or data used for polls or surveys; data stored data banks in connection with creditworthiness, assets and liabilities, appropriate performance of obligations, and unlawful and/or fraudulent conduct. Before the entry into force of the Code, the law provided the opposite principle: every processing operation should be notified, except those explicitly exempted from notification.

³³ See also Dec. 31 marzo 2004 in www.garanteprivacy.it [doc. web n. 852561](10.01.2009).

³⁴ See 2007 Annual report, pg. 197.

3.2. Appointment of staff in charge of the processing

- [50]. Beyond the obligations imposed by the DP Code on the data controller and on the data processor, processing operations may only be performed by persons in charge of the processing that act under the direct authority of either the data controller or the data processor by complying with the instructions received. They must be nominated in writing by specifically referring to the scope of the processing operations that are permitted.
- [51]. The Guidelines adopted by the Garante in respect of the employer-employee relationship³⁵ require that special importance must be attached to the identification of the entities that are entitled to process the data, by clearly setting out the respective powers (both for the data controller and the data processor). As for the staff specifically in charge of processing the employees' personal data, the Guidelines require that such staff has to receive proper training in network management and security, data protection principles, and communications secrecy. For SME's only [Small and medium enterprises], the simplification measures laid down in 2007 by the Practical Guidelines adopted by the DPA (see below Section 7), states that law requirements are met if a given employee is nominated as person in charge of the processing, provided the categories of data to be accessed by the said employee and the scope of the processing operations at issue are specified in writing. The Italian DP Code does not require for large-medium sized companies a specific role of internal legal counsel in charge of data protection.³⁶

³⁵ Italian Data Protection Authority, Guiding Principles Applying to the Processing of Employees' Personal Data for the Purpose of Managing Employment Relations in the Private Sector (23.12 2006), for details see below Section 4.5.

³⁶ See below Sections 6.5 and 6.8.

4. Sanctions, Compensation and Legal Consequences

4.1. Remedies: the alternative jurisdiction of the DPA and the courts

[52]. The DP Code has strengthened individuals' data protection rights, allowing them to exercise their rights and instigate proceedings more easily. Data subjects can settle disputes, alternatively, either through the courts or by lodging a complaint with the DPA in case they have been prevented from exercising access/erasure/updating rights (Article 7 of the Code). The DP Code provides for administrative, non-judicial and judicial remedies. As for the administrative and non-judicial remedies, the Code provides for several remedies that data subjects can lodge before the DPA.

4.1.1. Administrative remedies

[53]. Among the administrative remedies are to be listed the claims and reports:

- The *reclamo* [claim] before the DPA (see Article 141): data subjects may apply to the DPA to lodge a circumstantial claim, in order to point out an infringement of the relevant provisions on the processing of personal data. The DPA may call upon the data controller to autonomously block the processing before ordering the necessary and appropriate measures or before prohibiting or blocking the processing.
- In the case that no circumstantial claim has been lodged, data subjects may lodge a *segnalazione* [report], in order to call upon the DPA to check up on the relevant provisions on the processing of personal data. The DPA may adopt the same measures following a claim submitted by the data subject, already described above.

4.1.2. Non-Judicial Remedies

[54]. One of the non-judicial remedies is the *ricorso* [complaint] before the DPA. According to Article 145 of the Code, data subjects may lodge a complaint with a view to establishing the specific rights provided for by the Code. In an effort to simplify the complaints process, the DPA has published a complaints form on its website. This type of complaint can only be lodged in case of partial or total

failure to exercise the rights granted to data subjects (rights of access, rectification, information, erasure, etc.); it represents an alternative approach to legal action in courts and allows data subjects to obtain quick decisions (within 60 days from the date on which the complaint was lodged). Thus the rights granted by the Code may be enforced either by filing a lawsuit or by lodging a complaint with the DPA. The two remedies are alternative and cannot be exercised simultaneously. In any case, lodging a complaint with the DPA is only permitted after a request has been made to the data controller or processor (*interpello preventivo*), and the time period provided for in Article 8 has expired, or else if the request has not been partly satisfied.

- [55]. The DPA may provisionally order either the partial or total blocking of some of the data, or the immediate termination of one or more processing operations. Then, having gathered the necessary information, the DPA orders with a reasoned decision, if the complaint is found to be grounded, that the data controller abstains from the unlawful conduct; the DPA shall also specify the remedies to enforce the data subject's rights and set a term for their implementation. If no decision on the complaint is rendered within 60 days, the complaint is regarded as dismissed. If any party has previously requested it, the DPA shall also set out the costs and office charges relating to the complaint as a lump sum either to be charged, also in part, to the losing party, or to be compensated for, also in part, on rightful grounds. The decision taken by the DPA shall be communicated to the parties within 10 days. The decision of the DPA or the tacit dismissal may be challenged by the data controller or the data subject before courts. In any case, the challenging shall not suspend enforcement of the decision.

4.1.3. Judicial Remedies

- [56]. As for the judicial remedies (Article 152), the procedure before the courts is quite simplified: the judicial authority decides on the case as a single-judge court and formalities are less rigorous. Competence over any disputes concerning application of the provisions of the Code, including those related either to provisions issued by the DPA with regard to personal data protection or to the failure to adopt such provisions, lies with judicial authorities. The relevant proceeding shall be instituted by filing a petition within 30 days of the date on which the said provision is communicated or tacitly dismissed, with the clerk's office of the court having jurisdiction on the data controller's place of residence. The court shall grant or dismiss the petition, in whole or partly, order the necessary measures, provide for damages, if claimed, and impose legal costs on the losing party. The judgment may not be appealed, however it may be challenged before the Court of Cassation (the last-instance court in the Italian judicial system).

4.2. Compensation payments and sanctions

- [57]. Failure to comply with the provisions of the Personal Data Protection Code involves the application of compensation payments, administrative sanctions and criminal sanctions.
- [58]. As far as civil liability is concerned, whoever causes damage to another as a consequence of the processing of personal data shall be liable to pay damages (Article 15 of the Code). The Code considers as liability for dangerous activities, which means that the person responsible of the damage has to prove that she has adopted all the necessary measures to prevent the damage. The Code shifts the burden of proof in the treatment of personal and sensitive data away from the individual and onto the person actually processing the data. In two decisions issued in 2003, the Court of Cassation ruled that non-pecuniary damage should be construed as a wide-ranging category including all cases in which there is violation of a value inherent to human beings, and among these the use of unlawful means in collecting personal data.³⁷
- [59]. Insofar as administrative sanctions are concerned, (Articles 161-166 of the Code), the Code provides that the DPA can impose different economic sanctions in cases of: not providing or providing inadequate information to data subjects; assigning personal data in breach of the Code; not submitting or submitting an incomplete notification; violation of the provisions relating to traffic data retention; failure to provide information or produce documents to the DPA. Still one of the major problems resting with the pecuniary sanctions that the Garante is empowered to levy is that they are far from being considered as heavy.³⁸ As for the criminal sanctions these are only decided by courts and can be burdensome.³⁹ An assessment of both kinds of sanctions will be dealt with in Article 6 (Analysis of deficiencies) of this thematic study.

³⁷ Italy/ Corte di cassazione, decisions no. 8827 and 8828 of 2003 (31.05.2003) available at <http://www.ricercagiuridica.com/sentenze/index.php?num=394> (07.01.2009) and <http://www.federalismi.it/AppOpenFilePDF.cfm?dpath=document&dfile=31052006094706.pdf&content=Corte+di+Cassazione,+Sentenza+n.+8828/2003,+In+materia+di+danno+biologico+fisico+o+psichico+---+---+> (07.01.2009).

³⁸ As for Articles 161-166 of the Code, these are infringements that lead to administrative sanctions: *providing no or inadequate information to data subjects* (payment 3.000/18.000 euro; if sensitive or judicial data are involved 5.000-30.000); *Assigning personal data in breach of the Code* (5.000-30.000 euro); *Submitting no or an incomplete notification* (10.000-60.000 euro); *Punishments Applying to Traffic Data Retention*: Euro 10.000 to 50.000; *Failure to provide information or produce documents to the Garante* (4.000-24.000 euro).

³⁹ Criminal offence, according to Articles 167-170 of the DP Code, are considered: processing data unlawfully, with a view to gain for oneself or another or with intent to cause harm to another (imprisonment 6-18 months or, if the offence consists in data communication or dissemination, 6-24 months imprisonment; it is criminally irrelevant if minimal harm is caused to the individual's personal identity and privacy); disclosing sensitive data or personal data, for reasons differing from those notified to the Garante (3 months – 2 years

4.3. Follow-up of the *ex officio* surveys

- [60]. In recent years infringements of personal data protection provisions have been increasingly identified by the Data Protection Authority through investigations, initiated on its own motion rather than following claims or complaints lodged by citizens, associations, trade associations and professional rolls. These investigations have turned out to be, in many cases, also more effective than the complaints lodged by individual citizens as they focused on a growing number of issues that are broader in scope as well as on major areas of societal life and the activities of both public and private databases. The DPA's inspection powers are laid out in Article 158 of the Code. When investigating organisations, the DPA can request information and documents, although these requests are not legally binding. However, if there is no cooperation, and the organisations refuse access to its systems, the DPA can apply for a judicial order to carry out an investigation. When carrying out formal inspections, the DPA can demand copies of manual records and databases, which are then passed onto the judicial authorities.⁴⁰ The DPA can also order businesses to abide by compliance requirements set out in its decisions. When responding to investigations, businesses now have 15 days to comply, compared to the previous 5-day timeframe. A report of the outcome is then published.
- [61]. Special attention has been paid by the DPA to enforcement activities since 2005. This applies, in particular, to inspections and investigations in several sectors. Compared to years 2000-2004, in which they were very few (ranging between 20 and 69 inspections, see Annex 1), since 2005 they have significantly increased: 230 on-the-spot inspections were carried out in 2005 all over Italy. Inspections and controls increased from 350 in 2006 to 452 in 2007, thus leading to a 30% increase in inspections compared to 2006.⁴¹ This was made possible partly because of the development of innovative working methods on the basis of six-month inspection plans developed by the DPA, and

imprisonment); not informing the Garante of the data handling operations (imprisonment up to 1 year); failure to adopt the necessary measures to guarantee the security of handled data (imprisonment up to two years or a fine consisting in payment between 10.000 and 50.000 euro; within 60 days, the offender shall be permitted by the DPA to pay one-fourth of the highest fine that can be imposed in connection with the offence, if relevant requirements have been complied with: compliance and payment shall extinguish the offence); Untrue Declarations and Notifications Submitted to the DPA are punished by imprisonment for between six months and three years (Article 168), whereas failure to comply with the Guarantor's provisions is punished with a prison sentence ranging from three months to two years (Article 170).

⁴⁰ According to Article 158 of the Data Protection Code, the Garante may order that data banks and filing systems be accessed and audits on the spot be performed as regards premises where the processing takes place or investigations are anyhow to be carried out with a view to checking compliance with personal data protection regulations.

⁴¹ See Annual Reports for 2005, 2006 and 2007 of the Italian Data Protection Authority, available at:

<http://www.garanteprivacy.it/garante/navig/jsp/index.jsp?folderpath=Attivit%20+dell%27Autorit%20%2FRelazioni+annuali+al+Parlamento> (07.01.2009).

partly because of the signing in 2005 of an ad hoc Memorandum of Understanding between the DPA and Italy's *Guardia di Finanza* [Financial Police], a police specialised corps in charge of supervising compliance with taxation and financial legislation in Italy. Based on this Memorandum, the DPA may avail itself of staff from the Financial Police to carry out inspections, under its own instructions, in particular at local level. Thus the Financial Police was entrusted with the power of checking compliance with the requirements concerning notification, information notices, security measures and enforcement of the resolutions decided by the DPA.

- [62]. The inspections carried out in the recent years concerned primarily private entities and were aimed at checking compliance with the main requirements laid down in the data protection legislation. In 2005 they referred to telephone traffic data retention, the use of loyalty cards, credit reference agencies, personnel recruitment and the processing of personal and sensitive data by healthcare agencies. In 2006, inspections focused on the processing of personal data by credit reference agencies, the processing of medical data by pharmaceutical companies and healthcare bodies, the online processing of personal data, and the processing aimed at the provision of goods and services via distance selling mechanisms. This inspection activity led to ever growing results in the last years.⁴² In 2005 around 100 breaches of the data protection legislation were found. In 2006, following the inspections, 158 proceedings were set up in order to impose administrative sanctions; in 11 cases criminal information was referred to judicial authorities. Criminal sanctions concerned non-compliance with resolutions adopted by the DPA, failure to take minimum-security measures and the violation of the prohibition against the remote monitoring of employees. The administrative sanctions imposed amounted in 2006 to nearly Euro 600.000. Notified administrative breaches rose from 158 in 2006 to 228 in 2007; the decrees imposing fines and/or penalties went from 32 to 45, whilst the criminal breaches reported to judicial authorities rose from 11 in 2006 to 15 in 2007. In 2007 the sums levied in connection with fines imposed directly by the DPA amounted to Euro 814.625, whilst Euro 185.000 were levied to extinguish offences related to non-compliance with security measures. These figures are especially significant if one considers that the pecuniary sanctions the DPA is empowered to levy are far from heavy.

4.4. Effectiveness of personal initiatives of data subjects

- [63]. In Italy enforcement of data protection legislation does not depend primarily on personal initiative of data subjects, as many sanctions are imposed by the DPA

⁴² All figures were taken by official sources: Annual Reports for 2005, 2006 and 2007 of the Italian DPA. See also Annex 1.

following its own-motion investigations. In any case, the DPA provides expert assistance to data subjects, as the following figures concerning its activity demonstrate (all figures were taken from the Annual Reports submitted to the DPA to the Parliament).

- [64]. In 2005 the DPA replied to 1.633 claims and reports and to 364 requests for information or clarification.⁴³ In 2006, the DPA handled 2.717 reports and claims, while 679 queries were dealt with. In 2007 a remarkable increase in the replies to claims and reports, which rose from 2717 in 2006 to 3078 in 2007, shows the growing number of issues that are broader in scope whilst advisory and guidance activities were also on the rise. Reference should be made additionally to the work done by the citizens' bureau, which had to deal with several thousands of phone calls and e-mails. Special importance should be also given to the 135 replies provided in 2007 to questions related to the processing of sensitive and/or judicial data. The work done by the DPA in recent years thus shows a new trend, aiming at taking preventive measures in order to protect rather than step in at a later stage to punish. This is why the DPA continued its work concerning guidelines and strengthened its advisory and guidance activity in order to address the main issues coming from the individual sectors, foster good practices, and highlight the most frequent errors.
- [65]. As for legal assistance and representation in data protection cases, NGOs or associations do not play an important role because individuals can easily submit their claims before the DPA by means of an electronic format available on website. As far as judicial remedies are concerned, the DPA has locus standi in proceedings lodged before courts, if the case at stake concerns the lawfulness of a decision adopted by the DPA with a view to establishing the public interest. In this respect, the Peppermint case concerning the peer sharing of music files can be mentioned.⁴⁴ The financial risk of legal procedures in data protection cases (court fees, fees of attorney) lies with the losing party, to whom legal costs are charged by the courts; fees can also be compensated between the parties, also in part, on rightful grounds. It must be pointed out that, as in civil cases there is an inversion of the burden of proof (see above paragraph 30), the risks mainly resting with the data processor.

⁴³ Official source: see Annual Reports for 2005, 2006 and 2007 of the Italian DPA.

⁴⁴ Italy/ Tribunale di Roma, IX sezione civile, decision of July 14/2007, *Techland Sp. Z O.O. and Peppermint Jam Records GmbH versus Wind Telecomunicazioni S.p.A.*, in which the Court stated that identity disclosure requests are unacceptable because of the protection afforded to the secrecy of electronic communications between private parties, which is granted by the Italian Constitution as a fundamental right. The decision is available at <http://iusreporter.blogspot.com/2007/09/peppermint-il-tribunale-di-roma-rigetta.html> (07.01.2009).

4.5. Workers' data protection

- [66]. Italy has granted high level of protection of workers' rights long before a comprehensive legislation on the subject was issued. Italy has several laws relating to workplace surveillance, some of them dating back to the 70s. Several provisions protect employees in the workplace, a community where it is necessary to ensure that data subjects' rights, fundamental freedoms and dignity are guaranteed.⁴⁵ To that end, employees are enabled to freely express their own personalities within the framework of mutual rights and duties; additionally, they are entitled to a reasonable protection of their privacy in personal and professional relationships alike. Data protection legislation must be applied jointly with sector-related rules concerning employer-employee relationships and the use of technologies in such sectors, where data protection legislation is either left unprejudiced or expressly referred to.⁴⁶
- [67]. Some sector-related rules that are left unprejudiced by the data protection Code provide for specific prohibitions and limitations, such as those laid down by the Workers' Statute in respect of distance monitoring. The article 8 of *Statuto dei lavoratori* [Workers Statute] prohibits employers from investigating the political, religious or trade union opinions of their workers, and in general, on any matter that is irrelevant for the purposes of assessing their professional skills and aptitudes. Moreover, the Italian Data Protection Code and the article 4 of *Statuto dei lavoratori* [Workers Statute]⁴⁷ forbid any form of remote surveillance by the employer, whether through hardware or software systems. For instance, it is illegal to systematically read and record employee's emails or the web-pages consulted by him. Such forms of remote surveillance are deemed an illegal invasion to the employees' privacy within the workplace. According to the Data Protection Code, processing must comply with data protection safeguards and must be carried out in accordance of the following binding principles: necessity, or data minimization;⁴⁸ fairness (meaning that the fundamental features of the processing must be disclosed to employees);⁴⁹ the processing must be carried out for specific, explicit, and legitimate purposes in compliance with relevance and non-excessive principles;⁵⁰ the employer must process the data "in the least intrusive way possible"; monitoring may only be

⁴⁵ See, Articles 2 and 41, paragraph 2, of the Italian Constitution; Article 2087 of the Civil Code; Article 2 of the Digital Administration Code enacted with the legislative decree no. 82 of 7 March 2005 as for the right to have the processing of data by electronic networks brought into line with respect for fundamental rights and freedoms and data subjects' dignity.

⁴⁶ Articles 113, 114, and 184 of the DP Code; see also Article 47, para. 3), letter b), of the Digital Administration Code.

⁴⁷ Italy/legge n. 300/1970 (20.05.1970) available at <http://www.comune.jesi.an.it/MV/leggi/1300-70.htm> (07.01.2009).

⁴⁸ Information systems and software must be configured by minimizing use of personal and/or identification data in view of the purposes to be achieved, according to Article 3, para. 5.2, of DP Code.

⁴⁹ Article 11, para. 1, letter a), of the DP Code.

⁵⁰ Article 11, para. 1, letter b), of the DP Code, para. 4 and 5.

performed by the entities in charge thereof and “be targeted to the risk area, taking account of data protection rules and, where relevant, the principle of secrecy of correspondence”.⁵¹ Moreover, the new DP Code has fully implemented Article 8, letter b), of the Council directive 95/46/CE which applies to the processing of sensitive data. Organisations processing sensitive data that wish to find an alternative to the somewhat unreliable issues of employee consent, can look at the exemptions laid out in Article 26 of the Code. For example, Article 26, para. 4, letter d), allows the processing of sensitive data without consent if necessary to meet obligations under employment law.

[68]. The DP Code has also incorporated a new legislative provision on recruitment (set out in law n. 276/2003) which applies to areas such as the processing of curriculum vitae (for example, candidates must be provided with a data protection notice), employment agencies, and job advertisements. When recruiting staff, businesses are prohibited from collecting data relating to religion, trade union membership, political beliefs, marital status, health status, ethnic origin etc. The only exemption to this rule is if the specific job requires that this type of data be collected. The DPA too has paid considerable attention to the employment sector and the business world, providing simpler and more effective data protection for workers: in deciding several complaints, it has recognised the right for the employee to access any document containing personal data in the employer’s possession and has protected employees in relation to the monitoring set up by employers or against the unlawful use of biometrics data at the workplace.

[69]. Following these cases, the DPA adopted guidelines in respect of the employer-employee relationship in the private and in the public sector and the use of Internet and e-mails at the workplace. Both acts have set up important provisions as they tackled work sectors new technologies have impacted considerably on, thus leading the DPA to act instead of Parliament, which would be in a better position to adequately tackle these problems by safeguarding freedom of enterprise and, on the other hand, employees' right to privacy. First of all, a unified set of guidelines applying to the collection and use of personal data by private sector employers was laid down by the DPA with a resolution issued on November 23, 2006, also following several requests for information and complaints lodged by employees, trade unions and trade associations. These guidelines clarified many debated issues.⁵² Guidelines applying to "Employer-Employee Relationships in the Public Sector" have then been enacted in 2007.⁵³ These general guidelines were then followed in March

⁵¹ Italy/Garante per la protezione dei dati personali, Opinion n. 8 of 2001, points 5 and 12.

⁵² See Garante per la protezione dei dati personali, *Guiding Principles Applying to the Processing of Employees' Personal Data for the Purpose of Managing Employment Relations in the Private Sector* (23.11.2006) [doc. web no. 1427027], available at www.garanteprivacy.it (10.01.2009).

⁵³ See Garante per la protezione dei dati personali, *Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico*

1, 2007 by an additional, more specific resolution containing guidelines addressing the use of e-mail services and Internet in the employment context.⁵⁴

[70]. The guidelines set forth the principle that prevention should be more important than detection; in other words, that the interest of the employer is better served by preventing email and internet misuse rather than by simply detecting such misuse. For these reasons the DPA recommended the drafting of a comprehensive company policy, clearly and accurately stating the rules for the use of email and internet in the workplace. Specific guidelines aimed at clarifying the distinction between email use for professional and for private reasons and at regulating internet use in the workplace and specifically the monitoring of employees' access to internet were adopted. As for the role that the trade unions have in Italy in monitoring compliance with the applicable legislation in the data protection sector, it must be taken in due account that negotiation with trade unions is particularly important when undertaking surveillance of employees. More generally trade unions play a significant role in negotiating collective agreements. Collective bargaining can regulate all aspects of the employer-employee relationship, privacy and data protection included. Most categories of workers (roughly 95 per cent) in Italy are covered by a collective agreement.

(14.062007), in *Official Journal* of July 13, 2007, n. 161,[doc. web n. 1417809], available at www.garanteprivacy.it (10.01.2009).

⁵⁴ See Garante per la protezione dei dati personali, *Guidelines Applying to the Use of E-Mails and the Internet in the Employment Context* (01.03.2007), [doc. web no. 1408680], available at www.garanteprivacy.it (10.01.2009).

5. Rights Awareness

- [71]. We did not find any recent studies and surveys on awareness regarding data protection law and we are waiting for an answer from the DPA (we sent an e-mail the 21st of December, 2008).

6. Analysis of deficiencies

6.1. Deficiencies

- [72]. Deficiencies in data protection might be envisaged in the following areas: a) safeguards for public databases (especially for police databases and those serving national and State interests), which need to be listed in order to accomplish how many large-sized public databases are in existence and what types of database are available; b) relationships between media and data protection (especially in case of dissemination by the media of data originally collected for judicial purposes through the publication of wiretapping contents); c) level of data protection assured by judicial and legal practitioners in courts and in the business sector; d) powers of the DPA (especially inspection and sanctioning/injunction powers, which need to be boosted).

6.2. Exemptions

- [73]. The Italian data protection legislation has a very wide scope of application. However, ad hoc regulation is still lacking in regard of biological samples and DNA identification codes. The Data Protection Code currently requires an ad-hoc authorisation, which was recently issued by the DPA, to regulate the collection, processing and storage of DNA samples, in particular for scientific and/or research purposes. Still, there is no legislation applying to DNA processing in the fields of security and justice.
- [74]. In 2006 the DPA made on-the-spot inspections on the data processing operations carried out by a special investigation unit *Reparti Investigazioni Scientifiche* (RIS) of the *Carabinieri*, based in Parma. This inspections allowed the DPA to find out that this special unit had allegedly set up a database containing genetic information (gene samples and codes) taken from crime scenes, to be used for judicial investigations. Thus, there is an urgent need for legislation that provides for a suitable legal basis for activities that are currently out of all control: this is necessary also in view of implementing the Treaty of Prüm, whereby each EU Member State is expected to set up its own genetic database.

6.3. Required interventions

- As to the safeguards of databases, deficiencies could be overcome by adopting the organisational and security measures provided by the DPA, which would require huge financial resources. An important improvement would be the appointment of in-house privacy officers in charge of managing the security measures of the database and the relationship with the DPA. Moreover some legal provisions of the Data Protection Code still need to be implemented such as those requiring some Ministries to list the existing databases that are in operation for judicial and security purposes. The DPA reiterated several times this request to those authorities: in its view that list should be the first step in view of creating an ad-hoc "Registry of high-risk databases" which would also ensure increased transparency towards citizens.⁵⁵
- As to the deficiencies concerning the relationship between media and data protection, amending legislation should be taken into account and this might cover both the institutional framework of bodies protecting personal data, privacy as well as the sanctioning powers. In particular it might be envisaged a legislative amendment so as to allow the DPA to impose pecuniary administrative sanctions whenever it is ascertained that the rules set out in the Journalists' Code of Practice have been infringed. The DPA, as well, suggested the idea that new legislation could entrust it with the power to impose, in equity, compensatory damages subject to the parties' acceptance and additionally, that it might order that the relevant decision be published in a manner commensurate to that of the original piece of news.⁵⁶
- A legal regulation regarding the use of wiretapping contents and their publication is urgently needed in order to state whether and to what extent information gathered during the pre-trial investigations can be disclosed to the public, even before the trial has started. More effective legal constraints are needed. Still, it's not only a matter of amending legislation as the use of wiretapping transcripts also depends on the conduct of other entities, especially legal practitioners and judges. Thus, more suitable technical safety measures should be put in place: the DPA recommended to judicial offices specific instructions like carrying out tapping activities in a single location, encrypting their communications with telecom operators, taking technical measures aimed at logging data access, and strictly limiting the range of people entitled to access this information. The bill on interceptions currently under examination in Parliament, although it imposes heavy criminal sanctions on journalists who publish leaked extracts, regrettably does not provide any specific obligation to take specific technical measures to protect data gathered during wiretapping activities.

⁵⁵ See, along the same lines, the Italian Data Protection Authority, Annual Report for 2005.

⁵⁶ See Italian Data Protection Authority, Annual Report for 2006.

- As far as data protection in Courts is concerned, the enhancement of protection measures will mainly require the *Ministro della Giustizia e il Consiglio Superiore della Magistratura* [Minister of Justice and the Italian Higher Council of the Judiciary] to intervene by setting out specific organisational steps. Organisational difficulties, lack of resources and understaffing were the main obstacles to the adoption of the safety measures required several times by the DPA, and this necessarily requires the Parliament and the Government to allocate the necessary resources to the judicial authority.

[75]. In the business sector large and medium-sized companies should avail themselves of privacy officers. To this respect, regulatory amendments should be envisaged, so that the Italian DP Code provides the binding appointment of these officers in those companies.

[76]. Regulatory amendments to the DP Code are necessary both in order to increment the staffing of the Office and to boost inspection, sanctioning and injunction powers. The Garante also expressed the need that the Parliament considers establishing appropriate “fora” and mechanisms to ensure the continued dialogue with the DPA, an independent authority which has the Parliament as its reference counterpart.

7. Good practices

[77]. As far as the legal framework is concerned, the Italian legislation on Data Protection provides for very high standards of guarantee and covers a wide-ranging scope of application, including the press and media sectors.

- *Role played by the DPA* – The Italian DPA has played so far a very dynamic and proactive stance. Besides receiving and promptly reacting to reports and complaints, it is used to act ex officio in order to ban unlawful or unfair data processing operations. Good practices worth noting are the development of innovative working methods on the basis of six-month inspection plans developed by the DPA, and the cooperation with police bodies since 2005, when ad hoc Memorandum between the DPA and Guardia di Finanza [Financial Police] was signed. After adopting these instruments, investigations has significantly increased: from 230 in 2005 and 350 in 2006 to 452 in 2007, thus leading to a 30% increase in inspections compared to 2006.⁵⁷
- *Guidelines and “prior checking” in order to facilitate compliance* – In order to enhance an effective protection of privacy rights, DPA privileges and prefers preventive measures to ex post measure aimed at punishing violations. To this purpose DPA has enacted many Guidelines addressing individually the main sectors, in order to foster the good practices and highlight the most frequent errors. It has also boosted the preliminary assessment of data processing operations that require special precautions (“prior checking”), in particular when they involve sensitive or judicial data.⁵⁸ In order to adopt broad ranging-provisions in developing data protection guidelines, especially on highly sensitive sectors, the DPA

⁵⁷ See Annual Reports for 2005, 2006 and 2007 of the Italian Data Protection Authority, available at:


<http://www.garanteprivacy.it/garante/navig/jsp/index.jsp?folderpath=Attivit%E0+dell%27Autorit%E0%2FRelazioni+annuali+al+Parlamento> (09.01.2009)

⁵⁸ Among the most relevant guidelines, the practical guidelines for SME's, on employer-employee relationships in both private public sector, on customer relations in the banking sector, on publishing and disseminating documents and by local authorities, on data processing within the framework of clinical drug trials, on loyalty cards: [Guiding Principles Applying to the Processing of Employees' Personal Data for the Purpose of Managing Employment Relations in the Private Sector - 2006 november 23](#) (09.01.2009); [Guidelines Applying to the Use of E-Mails and the Internet in the Employment Context - 1 March 2007 \[1408680\]](#) (09.01.2009); [Guidelines for the Processing of Customers' Data in the Banking Sector - 25 ottobre 2007 \[1478096\]](#) (09.01.2009); [Guidelines for Data Processing within the Framework of Clinical Drug Trials - 2008 July 24 \[1544272\]](#)(09.01.2009) ; Guidelines for data processing by justice and court-appointed experts [/Linee guida in materia di trattamento di dati personali da parte dei consulenti tecnici e dei periti ausiliari del giudice e del pubblico ministero - 26 giugno 2008 \[1534086\]](#) (09.01.2009); [Loyalty cards and safeguards for consumers: guidelines applying to loyalty programmes - February 24, 2005 \[1109624\]](#) (09.01.2009).

launchs public consultations by calling on consumer associations, trade associations, providers of electronic communications services, citizens to give their views on key points.⁵⁹

- *Codes of practice* – A key feature of the Italian legal framework on data protection is the presence of several specific codes of practice, a flexible type of self-regulation, which is well suited for the requirements and specific features of the sectors concerned.⁶⁰ Among the several codes of practice adopted in the past years, the most well known is the Code of conduct applying to journalistic activities, adopted in 1998⁶¹ by the *Ordine dei giornalisti* [Board of Journalists], the official body representing Italian journalists, in co-operation with the DPA.
- *Simplification* – According to the criteria set out in Article 2 of the DP Code, whereby simplification is mentioned as a fundamental component of sound data protection provisions, several measures have been enacted recent ly in order to simplify existing regulation on data protection, by suppressing cumbersome procedures and excessive costs for citizens and business actors. Special attention has been paid to SMEs (small and medium enterprises), for which in 2007 the DPA adopted the "Practical Guidance and Simplification Measures for SMEs".⁶² Other important simplification measures adopted in 2007 concerned the processing of personal data by insurance companies and the mechanisms for customer care staff to inform users. In December 2008 simplification measures were taken for notifications and security measures.⁶³
- *High level of data protection for workers* – Italian legislation has always set high standards of protection for workers ever since the 70s. In that year Parliament passed the *Statuto dei lavoratori* [Workers Statute]:⁶⁴ article 8

⁵⁹ See, in particular for their relevance, the public consultations launched by the Garante in December 2004 regarding loyalty programmes; interactive TV, Radio Frequency Identification technology and videophones, and the one launched with a resolution on September 19, 2007 regarding “Measures and arrangements to safeguard data subjects in connection with the retention of telephone and internet traffic data for the detection and suppression of criminal offences”.

⁶⁰ Codes of practice on the processing of personal data: in the exercise of journalistic activities, for historical purposes; for statistical purposes within the framework of the Si.sta.n. [national statistical system]; for statistical and scientific purposes; Code of conduct and professional practice applying to information systems managed by private entities with regard to consumer credit, reliability, and timeliness of payments. All the codes of practices adopted are attached to the DP Code, available on the Italian Data Protection website (Data Protection Code ).

⁶¹ Code of conduct applying to journalistic activities, adopted on 29th July 1998, published in *O.J.* 3 August 1998, n. 179 (for the original Italian version see: [Allegato A.I. Codice di deontologia - Trattamento dei dati personali nell'esercizio dell'attività giornalistica](#) (09.01.2009)

⁶² [PRACTICAL GUIDELINES AND SIMPLIFYING MEASURES FOR SMEs \[1435985\]](#) (09.01.2009); A checklist is also provided in addition to the guidelines.

⁶³ Italian Data Protection Authority, *Semplificazione delle misure di sicurezza* [Simplification of minimum security measures],((27.11.2008) [doc. web n. 1571218], www.garanteprivacy.it (10.01.2009).

⁶⁴ Italy/legge n.300/1970 (20.05.1970).

prohibits employers from investigating the political, religious or trade union opinions of their workers, and in general, on any matter that is irrelevant for the purposes of assessing their professional skills and aptitudes. The Italian Data Protection Code and the Workers Statute (Articles 4) forbid any form of remote surveillance by the employer, whether through hardware or software systems.⁶⁵

- *Measures for raising awareness regarding data protection law and rights and for spreading the culture of data protection* – Data controllers are required to adopt the so-called *Documento programmatico sulla sicurezza-DPS* [security policies document], a compulsory instrument aimed at affording workers, citizens, users, and consumers the protection of fundamental individual rights. The adoption of the security policy is regarded as a push for all stakeholders to spread the culture of privacy.⁶⁶ The form for exercising and enforcing the rights granted by the DP Code has been published on the website of the DPA, in order to help citizens. The DPA has constantly promoted institutional communication on data protection: there is a weekly newsletter that has been published since 1999 to provide the public with information on the DPA’s activities and also a six-monthly CD-ROM containing a digital archive of the DPA’s activities plus the reference legislation. In addition, the Authority has held training programmes (in-house workshops) on the features or application issues related to the Data Protection Code as addressed to private and public data controllers. Recently, the DPA promoted the use of graphical symbols to facilitate understanding of the personal data are at issue (a closed padlock and an open padlock, respectively, to signify that the data must be processed exclusively for the purposes for which the data has been provided and to allow using the data for other purposes, which must be specified in an ad-hoc information notice). Specific communication initiatives were launched with particular regard to youths (among these, the Garante together with the *Ministero dell’Istruzione* [Ministry of Education] drew up Guidelines for the appropriate use of cellphones and their video cameras during school classes).

⁶⁵ See for the Italian version of the Workers Statute, Italy/legge n.300 (20.05.1970): http://www.italgiure.giustizia.it/nir/lexs/1970/lexs_225234.html (09.01.2009)

⁶⁶ The Italian Data Protection Authority provided a Guide for the preparation of the “security policies” <http://www.garanteprivacy.it/garante/document?ID=1007740> (28.12.2008).

8. Miscellaneous

[78]. NTR

Annexes

Annex 1 – Tables and Statistics

YEARS	2000	2001	2002	2003	2004	2005	2006	2007
Budget of data protection authority (in Euros from State)	11.385.29,34	11.362.051,78	10.849.996,00	10.252.000,00	9.618.000,00	9.540.653,00	19.600.00,00	18.777.293,72
Staff of data protection authority	Managers: 19 Officers: 21 Staff: 11 Workers contract: 20 by	Managers: 19 Officers: 25 Staff: 14 Workers contract: 11 by	Managers: 23 Officers: 33 Staff: 20 Workers contract: 15 by	Managers: 22 Officers: 33 Staff: 20 Workers by contract: 18	Managers: 20 Officers: 40 Staff: 22 Workers by contract: 12	Managers: 18 Officers: 38 Staff: 21 Workers by contract: 14	Managers: 17 Officers: 43 Staff: 21 Workers by contract: 9	Managers: 17 Officers: 46 Staff: 23 Workers by contract: 13

YEARS	2000	2001	2002	2003	2004	2005	2006	2007

YEARS	2000	2001	2002	2003	2004	2005	2006	2007
Number of procedures (investigations, audits etc.) initiated by data protection authority at own initiative: INVESTIGATIONS	20	18	40	69	not available	230	350	452
Number of procedures initiated by data protection authority at own initiative: REPORTS TO THE JUDICIARY AUTHORITY	4	7	5	16	16	7	11	15
Number of procedures initiated by data protection authority at own initiative: Request for information and for documents pursuant to Art. No. 32, 1 Italy/Legge 165/2003 to the right holder, to the guilty or to third	95	242	165	227	110	84	407	461

YEARS	2000	2001	2002	2003	2004	2005	2006	2007
persons								
Number of data protection registrations	295.000 (including some of the previous years)	17.500	12.227	9.791	10.081	11.905	2.397	978
Number of data protection approval procedures	Authorizations to individuals: 2 General Authorizations issued for data treatment: 7	Authorizations to individuals: 1 General Authorizations issued for data treatment: 22	Authorizations to individuals: 1 General Authorizations issued for data treatment: 7	Authorizations to individuals: 2 General Authorizations issued for data treatment: 7	Authorizations to individuals: 22 General Authorizations issued for data treatment: 7	Authorizations to individuals: 2 General Authorizations issued for data treatment: 7 Prior checking on treatments with risk of infringement upon data protection: 4	Authorizations to individuals: 2 General Authorizations issued for data treatment: 7 Prior checking on treatments with risk of infringement upon data protection: 7	Authorizations to individuals: 2 General Authorizations issued for data treatment: 7 Prior checking on treatments with risk of infringement upon data protection: 4

YEARS	2000	2001	2002	2003	2004	2005	2006	2007
Number of complaints received by data protection authority	243	211	500	775	731	634	435	316
Number of complaints upheld by data protection authority (petitions accepted or partially accepted)	30	30	176	228	208	114	66	45
Follow up activities of data protection authority, once problems were established (please disaggregate according to type of follow up)	Acts and measures adopted after recommendations or claims: 687	Acts and measures adopted after recommendations or claims: 2.327	Acts and measures adopted after recommendations or claims: 3.689	Acts and measures adopted after recommendations or claims: 4.080	Decisions issued by the Committee: 724 Replies to claims and	Decisions issued by the Committee: 769 Replies to claims and	Decisions issued by the Committee: 643 Replies to claims and	Decisions issued by the Committee: 495 Replies to claims and

YEARS	2000	2001	2002	2003	2004	2005	2006	2007
activity: settlement, warning issued, opinion issued, sanction issued etc.)	<p>Answers to questions: 118</p> <p>Opinions rendered to the Government when drawing up regulations and administrative measures liable to produce effects on data protection: 70</p>	<p>Answers to questions: 898</p> <p>Opinions rendered to the Government when drawing up regulations and administrative measures liable to produce effects on data protection: 27</p>	<p>Answers to questions: 1.003</p> <p>Opinions rendered to the Government when drawing up regulations and administrative measures liable to produce effects on data protection: 9</p>	<p>Answers to questions: 834</p> <p>Opinions rendered to the Government when drawing up regulations and administrative measures liable to produce effects on data protection: 14</p>	<p>reports: 3.595</p> <p>Answers to questions: 319</p> <p>Opinions rendered to the Government when drawing up regulations and administrative measures liable to produce effects on data protection: 10</p>	<p>reports: 906</p> <p>Answers to questions: 200</p> <p>Opinions rendered to the Government when drawing up regulations and administrative measures liable to produce effects on data protection: 22</p>	<p>reports: 2.717</p> <p>Answers to questions: 679</p> <p>Opinions rendered to the Government when drawing up regulations and administrative measures liable to produce effects on data protection: 13</p>	<p>reports: 3.078</p> <p>Answers to questions: 485</p> <p>Opinions rendered to the Government when drawing up regulations and administrative measures liable to produce effects on data protection: 16</p>
Sanctions and/or compensation payments in data protection cases (please disaggregate)	Orders of injunctions: 4	Orders of injunctions: 6	Orders of injunctions: 5	Not available	Pending cases notified to the Authority: 32	Administrative sanctions: 94	Orders of injunctions: 32	Orders of injunctions: 45

YEARS	2000	2001	2002	2003	2004	2005	2006	2007
between court, data protection authority, other authorities or tribunals etc.) in your country (if possible, please disaggregate between sectors of society and economy)						Pending cases notified to the Authority: 74	Administrative sanctions: 158 Pending cases notified to the Authority: 159	Administrative sanctions: 228 Pending cases notified to the Authority: 134
Range of sanctions and/or compensation in your country (Please disaggregate according to type of sanction/compensation)	Administrative fees: 25,82 Euros Reimbursement of expenses: 100,00 Euros maximum	Administrative fees: 25,82 Euros Reimbursement of expenses: 100,00 Euros maximum	Proceeds from payment of sanctions: 73.337 Euros Administrative fees: 25,82 Euros Reimbursement of expenses: 100,00 Euros	Proceeds from payment of sanctions: 20.142 Euros Administrative fees: 25,82 Euros Reimbursement of expenses: 100,00	Proceeds from payment of sanctions: 30.197 Euros Administrative fees: 25,82 Euros Reimbursement of expenses:	Proceeds from payment of sanctions: 644,00 Euros Administrative fees: 150,00 Euros Reimbursement of expenses:	Proceeds from payment of sanctions: 302.200 Euros Administrative fees: 150,00 Euros Reimbursement of expenses:	Proceeds from payment of sanctions: 814.625 Euros Administrative fees: 150,00 Euros Reimbursement of expenses:

YEARS	2000	2001	2002	2003	2004	2005	2006	2007
			maximum		100,00	500,00 Proceeds from data protection registration: 1.782.300,00 Euros	500,00 Proceeds from data protection registration: 359.550 Euros	500,00 Proceeds from data protection registration: 146.700 Euros

Official sources: Annual Reports of the Italian Data Protection Authority submitted to Parliament for years 2000-2007;
Direct interviews of the Italian Data Authority in November 2008.

Annex 2 – Case Law

Please present at least 5 cases on data protection from courts, tribunals, data protection authorities etc. (criteria of choice: publicity, citation in media, citation in commentaries and legal literature, important sanctions) in your country, if available (please state it clearly, if less than 5 cases are available).

Note: for full texts of the original decisions of the cases presented in this document please see Annex 3.

Case title	Case “Le Iene” – Medical data collected surreptitiously
Decision date	14th December 2006
Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	Provvedimento generale doc. web n. 1345622 / General provision doc. web n. 1345622 Garante per la protezione dei dati personali /Italian Data Protection Authority

<p>Key facts of the case (max. 500 chars)</p>	<p>An Italian TV channel wanted to broadcast a programme (“Le Iene” being the name of the said TV show) concerning a drug test performed on 50 MPs, in front of one of the Chambers of Parliament, without their being aware of. The intent of the programme by showing those medical data collected surreptitiously was to establish the alleged use of drugs by politicians contacted in front of the Lower House.</p>
<p>Main reasoning/argumentation (max. 500 chars)</p>	<p>The Garante prevented the TV broadcasting. The DPA found that medical data had been processed unlawfully in this case, especially by having regard to their collection, irrespective of the dissemination of such data via the TV programme. The persons concerned had not been informed about the explicit purposes of the processing, and their biological samples had been collected in a misleading, unfair manner. Based on these grounds, the Garante prohibited the collection, storage and use of the data in question.</p>
<p>Key issues (concepts, interpretations) clarified by the case (max. 500 chars)</p>	<p>The provision adopted by the DPA clarified that enhanced protection is necessary when you handle medical data, and that these data may be never be acquired deceitfully. It was actually even more important to explain how socially dangerous it can be to make use of fraudulent mechanisms to lay hands on biological samples concerning individuals, given the information that can be derived on their health and life expectancy. This danger is all the more serious nowadays, when the tests in question can become a large scale phenomenon and foster a highly risky "do-it-yourself" approach.</p>
<p>Results (sanctions) and key consequences or implications of the case (max. 500 chars)</p>	<p>The DPA adopted an administrative sanction: the order of blocking the use of medical data and the prohibition to collect, store and use of medical data without express prior consent of data subjects. Since then media are banned to broadcast medical data collected surreptitiously</p>
<p>Proposal of key words for data base</p>	<p>Medical data – lawful processing</p>

Case title	Case “Sircana” - Publishing Transcripts of Tapping Records
Decision date	21st June 2006
Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	Provvedimento generale doc. web n. 1301195 / General provision doc. web n. 1301195 Garante per la protezione dei dati personali / Italian Data Protection Authority
Key facts of the case (max. 500 chars)	The case concerned the repeated publication by several newspapers of transcripts of telephone wire tapings that had been ordered by judicial authorities, concerning several individuals. The transcripts published contained information on the sex preferences and life of several persons, both well-known and less well-known; there were people from the world of politics and entertainment as well as the man in the street, but all of them were somehow involved in the wiretapping activities carried out during judicial investigations.
Main reasoning/argumentation (max. 500 chars)	The Garante recalled the provisions in force and referred to the need for complying with the principle whereby only information that is material to the case must be published and no reference should be made to relatives or other individuals having no connections with the specific case; respect for human dignity should be paramount, and special safeguards are required in respect of the information concerning a person’s sex life.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	The Garante stressed the need for reconciling a citizen’s right to be informed and freedom of the press, on the one hand, with the respect for fundamental rights and freedoms of the individuals concerned on the other – particularly with their right to privacy. The reduced privacy expectation of public figures and/or holders of public offices must be reconciled with the journalist’s inescapable duty to protect human dignity and third parties’ rights.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The provision was addressed to all data controllers in the journalistic sector and published in the Official Journal. All media were called upon to perform a more careful, in-depth, autonomous, responsible analysis as to whether any details that are disclosed are actually material.
Proposal of key words for data base	Publishing of tapping transcripts – Human dignity – Public figures

Case title	Case “Taxpayers’ Lists on the Internet”
Decision date	6 Maggio 2008 / 6 May 2008
Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	Decisione 6 maggio 2008 [doc. web n. 1512255 , Italian version] (28.12.2008) / <i>Decision 6 May 2008 [English version, doc. web n. 1519208] (28.12.2008)</i> Garante per la protezione dei dati personali / <i>Italian Data Protection Authority</i>
Key facts of the case (max. 500 chars)	The Italian legislation applying to publication of the lists of taxpayers that have submitted tax returns provides that the lists are drawn up annually on that basis and deposited for 1 year with the individual municipalities and the geographically competent branches of the Revenue Office in order for anyone to browse them. The Italian Revenue Office, implementing the above requirements, decided that the lists, as for the year 2005, should also be posted in the ad-hoc section of the website managed by the Revenue Office <i>"with a view to browsing such lists"</i> .
Main reasoning/argumentation (max. 500 chars)	The DPA decided that the Italian Revenue Office posted the data relating to tax returns on the internet unlawfully because of the lack of an appropriate legal basis, preconditions and authorisations. The decision by the Director of the Revenue Office could only lay down the "terms and arrangements" for drawing up the taxpayers' lists. The blocking was also ordered because the data had been disseminated without safeguards to prevent search engines – any in the world – from getting, modifying or misusing those data.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	Access to taxpayers lists is regulated specifically by the law, whereby the only arrangements consist in circulating the lists to the geographically competent branches of the Revenue Office and forwarding such lists, either on magnetic media or via electronic networks, exclusively to the individual municipalities concerned; in both cases, the lists may only include the taxpayers that are resident in the respective geographic areas. This procedure is aimed at ensuring that the lists be deposited for one year in the manner described above and may be browsed – though not copied – by anyone (section 69(4) et seq. of Presidential decree no. 600/1973; see also section 66-bis of Presidential decree no. 633 dated 26 October 1972);

<p>Results (sanctions) and key consequences or implications of the case (max. 500 chars)</p>	<p>The decision blocked the posting on Internet of the data of all Italian taxpayers who submitted tax return forms for 2005 and prohibited the Revenue Office from disseminating the said lists further on the Internet; it also notified the Revenue Office of the commission of an administrative infringement because it failed to provide appropriate information beforehand to the taxpayers concerned and ordered the Office to ensure that this decision be publicized to the widest possible extent, also by having it published in the <i>Official Journal</i> of the Italian Republic.</p>
<p>Proposal of key words for data base</p>	<p>Tax returns – publication on Internet</p>

Case title	Case Videophones / MMS at the workplace
Decision date	5 December 2005
Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	Corte di cassazione (V sezione penale) / Court of Cassation (5th Division, Penal Matters) Sentenza n. 10444 del 5 dicembre 2005 / Judgement no. 10444 of 5 December 2005 <i>[Note: the Court of cassation is the last-instance court in the Italian judicial system]</i>
Key facts of the case (max. 500 chars)	A man with his videophone had taken many pictures of a lady at the workplace, without her consent, and persecuted her, and was convicted to jail accused of sexual harassment .
Main reasoning/argumentation (max. 500 chars)	Taking pictures with a videophone, including at the workplace, without the data subject's consent and/or without the data subject's being aware thereof, is an unlawful interference with private life.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	In the Court's view, Section 615-bis of the Italian Criminal Code is meant to punish unlawful interferences with another's private life as caused by technical implements that can reproduce the violation of privacy resulting from the disclosure of what is not meant for third parties' unrestrained perusal.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The Court of Cassation confirmed the penal sanction decided by the judge of first instance, that convicted to jail th man.
Proposal of key words for data base	Unlawful interference with private life – Videophones – MMS taken at the workplace

Case title	Case “Sensitive data processed by public authorities”
Decision date	8 luglio 2005 /8th July 2005
Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	Sentenza n. 14390 del 2005 / Decision no. 14390 of 2005 Corte di cassazione (I sezione civile) / Court of Cassation (1st Devision, Civil Matters) <i>[Note: the Court of cassation is the last-instance court in the Italian judicial system]</i>
Key facts of the case (max. 500 chars)	A police official had been suspended from office after he had been recognised in a hard-core picture on a website with “homosexual and feticist contents”. The police official had lodged a complaint with the DPA against use of the sensitive data taken from the pictures, which had been posted on the Internet, He alleged the conduct of the police had been unlawful, in particular because his colleagues (who had found the addresses of the websites visited by the official at the latter’s home and had subsequently proffered information on him) had acted outside their official duties.
Main reasoning/argumentation (max. 500 chars)	The decision recalled, according to Article 20, para. 2, of the Data Protection Code, the obligation for public bodies to adopt ad hoc privacy regulations on processing of sensitive and judicial data, specifying the sensitive data involved and the processing operations that can be performed by public bodies, which must rely on a careful assessment of the purposes pursued via the various processing operations as well as of the personal data that is actually required in order to lawfully treat personal data.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	The processing by public bodies of sensitive data (and especially the high level sensitive data concerning health and sexual life), even if aimed at adopting disciplinary sanctions (and thus for public interest ends) requires in any case the written consent by the data subject (the civil servant) if the law or the said public body have not detailed the processing operations and data categories involved.

<p>Results (sanctions) and key consequences or implications of the case (max. 500 chars)</p>	<p>The Court of Cassation ruled that the measure taken by the Ministry of Home Affairs against the police official was void and referred the case back to the competent court in order to establish whether the Ministry could lawfully process the highly sensitive personal data concerning the complainant.</p>
<p>Proposal of key words for data base</p>	<p>Sensitive data – Processing by public bodies</p>