**ITALY**

***Ministry of Foreign Affairs and International Cooperation***

*Inter-ministerial Committee for Human Rights*

*Comitato Interministeriale dei Diritti Umani*

**ITALY’S CONTRIBUTION AND SUBMISSION TO**

**THE STUDY ON SOCIAL MEDIA,**

**SEARCH AND FREEDOM OF EXPRESSION**

***March 2018***

**ITALY’S CONTRIBUTION**

*freedex@ohchr.org*

***Subject: Submission to Study on Social Media, Search, and Freedom of Expression***

Following your query, Italian Authorities are in a position to provide the following information:

**Introduction**

Freedom of expression and freedom of the press are protected by the Italian Constitution of 1948 in its Article 21, which reads: “Anyone has the right to freely express their thoughts in speech, writing, or any other form of communication. The press may not be subjected to any authorization or censorship [...]”.

On a more general note, the Basic Law determines the political framework for action and organization of the State. The fundamental elements or structural principles of the constitutional law governing the organization of the State are as follows: Democracy, as laid down in Article 1; the so-called *personalistic* principle, as laid down in Article 2, which guarantees the full and effective respect for human rights; the pluralist principle, within the framework of the value of democracy (Arts. 2 and 5); the importance of work, as a central value of the Italian community (Arts. 1 and 4); the principle of solidarity (Article 2); the principle of equality, as laid down in Article 3 (it is also the fundamental criterion applied in the judiciary system when bringing in a verdict); the principles of unity and territorial integrity (Article 5); and above all, the relevant principles, including the social state, the rule of law, and the respect for human rights and fundamental freedoms, such as freedom of correspondence, freedom of movement, freedom of religion or belief, and freedom of opinion and expression.

- The Italian legal system aims at ensuring an effective framework of guarantees, to fully and extensively protect the fundamental rights of the individual. Indeed, we rely on a solid framework of rules, primarily of a constitutional nature, by which the respect for human rights is one of the main pillars.

The Constitutional Court

Within our national system of protection of human rights, mention has to be made, among others, of the Italian constitutional court that deals only with infringements of a constitutional level (The constitutional court consists of fifteen judges; one-third being appointed by the President of the Republic/Head of State, one-third by the Parliament in joint session, and one-third by ordinary and administrative supreme court)[[1]](#footnote-1). The constitutional court exercises its duty as one of the highest guardian of the Constitution in various ways. It becomes active when it is called on. For example, it supervises the preliminary stages of referenda and is competent in case of presidential impeachment. Complaints of unconstitutionality may be submitted to the Italian Constitutional Court by central and local authorities claiming that a state or a regional Act might be unconstitutional. Therefore, the Court monitors Authorities to see whether they have observed the Constitution in their actions. It also arbitrates in cases of disagreements between the highest State’s organs and decides in proceedings between central and local authorities.

* Procedurally, the court must examine *ex officio* (the prosecutor) or upon request of the plaintiff/defendant whether the provisions to be applied are in compliance with the Basic Law. When the court considers that an act is unconstitutional, such evaluation brings to a suspension of the *a quo* proceeding. Accordingly, a decision is made by the Court itself, pursuant to Art. 134 of the Italian Constitution. The constitutional court decides (and its decisions cannot be appealed on) disputes: 1. concerning the constitutionality of laws and acts with the force of law adopted by state or regions; 2. arising over the allocation of powers between branches of government, within the state, between the state and the regions, and between regions; 3. on accusations raised against the head of State in accordance with the Constitution. More generally, this Court decides on the validity of legislation, its interpretation and on whether its implementation, in form and substance, is in line with the Basic Law. Thus, when the court declares a law or an act with the force of law unconstitutional, the norm ceases its force by the day after the publication of its decision.

Given the areas of the study under preparation, it is important to provide an overview of the role and work carried out particularly by AGCOM, standing for the Communication Regulatory Authority[[2]](#footnote-2) and the Italian DPA, standing for the Italian Data Protection Authority:

The Communication Regulatory Authority (acronym in Italian, AGCOM)

The Communication Regulatory Authority is an independent Authority, established by Act 249/1997. Independence and autonomy are key elements that characterize its activities and resolutions. AGCOM is first and foremost a guarantee Authority: its law of establishment entrusts the Authority with the double task of ensuring the correct competition of operators on the market and of protecting consumers' fundamental freedoms.

The Communication Authority is a "convergent" Authority. As such, it performs regulatory and supervisory functions in the telecommunications, audiovisual, publishing and, more recently, postal sectors. The profound changes brought about by the digitalization process, which has ensured the uniform broadcast of audio (including voice), video (including television) and data (including Internet access), are the basis for the choice of convergent model, as adopted by the Italian legislator and shared by other sector Authorities, such as Ofcom in Great Britain and Fcc in the United States.

Like the other Authorities provided for by the Italian legislation, the AGCOM report on its work to the Parliament. The latter established this Authority’s powers, defined the statute and elected the members (Authority's bodies are: the President, the Commission for infrastructures and networks, the Commission for services and products, the Council. The Commissions and the Council are collegial bodies. The Commissions are made up of the President and the two Commissioners. The Council is composed of the President and all the Commissioners).

On a more specific note, Act 215/2004[[3]](#footnote-3), which deals with the mass media and information sector and which covers possible conflicts of interest, including between government responsibilities and professional and business activities in general, details *inter alia* the powers, functions and procedures of the independent administrative Authorities responsible for oversight, prevention and imposing penalties to combat such cases, together with the applicable penalties:

* For companies in general, this responsibility lies with the Anti-trust Authority established by Act 287/1990 (Art. 6);
* For companies of the printed press and media sector, the responsibility lies not only with the above Authority but also with AGCOM, as instituted by Act 249/1997.
  + The above Authorities are characterized by their neutrality with regard to the parties with conflicting interests to be resolved and third parties, and are therefore *iusdicenti* in any relevant conflicts. Specifically, Act 215/2004 entrusts AGCOM to conduct audits against companies operating in the Integrated Communications System (acronym, SIC) and are headed by the holder of governmental position (or by relatives).

* + - The SIC comprises all the main media business sectors, and may be considered to be the result of the multimedia convergence process in which apparently heterogeneous media (radio, television, newspapers, the Internet, cinema) are gradually drawing closer together and becoming integrated[[4]](#footnote-4).

As for RAI, the public broadcasting service, a parliamentary commission ensures, inter alia, respect for pluralism. It is, however, AGCOM to oversee and ensure RAI’s compliance with primary and secondary level provisions, with regard to pluralism and public service-related obligations.

AGCOM has been also entrusted with all those functions of a regulatory and control nature, relevant to the postal sector, in accordance with Art.1, paras.13 and 14, of Law Decree No. 201/2011, as converted into law (with amendments) by Act No. 214/2011.

With regard to intellectual property, AGCOM has introduced rules on the protection of copyright by Resolution (No.680/13/CONS), dated December 12, 2013, by which it identifies its jurisdiction in respect of those breaches occurring on electronic communications networks in accordance with Legislation on Copyright (Act No. 633/41 - in particular Article 182 bis, by which both this Authority and SIAE are entrusted, within their respective responsibilities, with supervisory powers) and Legislative Decree on Electronic Trade (Act No.70/2003 - entrusting AGCOM with the power to order the intermediary service providers to put an end to the violations committed in the network).

* With specific regard to the audiovisual media services, it should be stressed that Parliament has entrusted the above Authority with specific regulatory and normative powers in accordance with Art.32bis of Legislative Decree No. 177/2005 (entitled "Consolidated Text on Audiovisual and Radio Media Services").

The Italian DPA

The *Garante*, i.e. the Italian Data Protection Authority (DPA), is an administrative independent authority set up by the "Privacy Act" (675/1996, now merged into the consolidated Personal Data Protection Code).

- Similar authorities have been set up in all EU countries pursuant to Article 8 of the Charter of Fundamental Rights of the European Union.

The *Garante* is tasked with ensuring the protection of fundamental rights and freedoms as regards the processing of personal data along with respect for individuals' dignity. The *Garante* handles citizens' claims and reports and supervises over compliance with the provisions protecting private life. It decides on complaints lodged by citizens and is empowered to prohibit, also of its own motion, any processing operation that is unlawful or unfair. It can perform inspections, impose administrative penalties, and issue opinions in the cases mentioned by the Data Protection Code. It can also draw Parliament's and Government's attention to the desirability of regulatory measures concerning personal data protection.

**Specific Issues**

AGCOM

As earlier mentioned, the main activity carried out by AGCOM with regards to content online is the adoption of Decision No.680/13/CONS, which introduces a specific procedure aimed at fighting online piracy. This was an unprecedented measure, which created a brand new tool, managed by AGCOM itself, to boost the protection against breaches to copyright perpetrated by online platforms or services: the procedure is launched when a complaint is filed by the right-holders, who claim that a work belonging to them has been published against the copyright provisions; all interested parties (e.g. internet service providers, uploaders, page/site owners) are then invited to participate to the procedure and present relevant documentation.

When, on the basis of the documents received by the parties, AGCOM detects an actual infringement of the copyright law in the online environment, it may adopt different measures depending on the location of the server hosting the content:

* If the server is located in Italy, AGCOM may order the hosting provider to remove the digital work from the website and show a notice containing an indication about the copyright violation;
* If the server is located outside of Italy, although AGCOM may not order the selective removal of the illegal content, as this would imply deep packet inspections and thus be against EU law, AGCOM may order access providers established in Italy to disable the access to the website disseminating illegal content, by blocking the DNS resolution or the IP address.

The deadlines of this procedure are quite tight: AGCOM is bound to provide a decision within 35 working days, which are reduced to 12 in some special cases (outstanding economic value of the work, reiteration of the same case, and so on).

Obviously, the procedure before AGCOM does not replace the judicial process, and it freezes in the event of an appeal of either party to the Court. As all AGCOM decisions, the decisions regarding copyright can be challenged before the Administrative Regional Tribunal-TAR Lazio (the Administrative Court).

In the first 3 years since the entry into force of the Regulation, AGCOM has received 729 complaints[[5]](#footnote-5)[1], excluding those ones, which have been withdrawn or never completed.

It is worth-recalling that only complaints from the effective right-holders or subjects entitled to represent them can be accepted. In 429 cases, the procedure ended with a removal of the content from the platform/website, either voluntarily from the ISP or after a specific order from AGCOM (in 277 cases).

In addition to online copyright regulation, in the last years AGCOM has been very active in monitoring the role of the largest Internet platforms (including social networks, search engines and other online intermediaries) in the Italian news media system.

It has to be preliminarily clarified that neither the EU nor the national legal framework clearly define online platforms (including social media, search platforms and/or platforms users) as “communications operators” subject to the AGCOM regulation.

However, online platforms fell under the AGCOM’s scrutiny in the context of the evaluation of the total revenues of the Integrated Communications Systems (Italian Acronym: SIC). Such evaluation is performed by AGCOM, as requested by Article 43 of the Italian Audio-Visual Media Act (Law No. 177/2005 as amended in 2012), and involves an assessment of the online advertising market where the major global platforms, such as Google and Facebook, account for a significant share of revenues[[6]](#footnote-6).

The evaluation of the SIC total revenues is essential to perform the AGCOM institutional functions aimed at safeguarding pluralisms and competition in the audio-visual sector by assessing dominant positions in the relevant markets.

It is worth-noting that although Google had challenged the AGCOM decision, the Italian Administrative Court (*TAR Lazio*) has ruled against the platform by pointing out that safeguarding pluralism justifies enhanced competition regulation in all relevant communications markets, including online advertising[[7]](#footnote-7).

Furthermore, AGCOM recognizes that the rise of online platforms and their impact on disinformation require a profound rethinking of the existing regulatory framework pursuing the objectives of fair competition, media pluralism, and protection of fundamental rights of Internet users, and it is currently promoting voluntary approaches and cooperation with online platforms to safeguard pluralisms and fair information in the online news media system.

In November 2017, by adopting its Decision 423/17/CONS, AGCOM established the *“Tavolo tecnico per la garanzia del pluralismo e della correttezza dell’informazione sulle piattaforme digitali”*, with the aim of promoting self-regulation and the exchange of good practices in detecting and tackling online disinformation arising from targeted strategies.

The “*Tavolo tecnico*” is made of four different roundtables: online platforms (Facebook, Google, Wikipedia, Twitter, Qwant); Publishers; Journalists’ organisations and Advertisers[[8]](#footnote-8)).

DPA

Of relevance is the role played by the Italian DPA, standing for Italian Data Protection Authority (*Garante per la protezione dei dati personali*). It is an independent authority set up to protect fundamental rights and freedoms in connection with the processing of personal data, and to ensure respect for individuals' dignity.

The DPA was set up in 1997, when the former Data Protection Act came into force. It is a collegiate body including four members, who are elected by Parliament for a seven-year term. The authority has an office in Rome with a staff currently numbering about 125 people. The Collegiate Panel of the Italian DPA is currently composed of: one President; one Vice-President; two more members; and one Secretary-General to the DPA.

The Data Protection Code 196/2003, which superseded the Data Protection Act 675/1996, defines DPA’s tasks. They include the following: supervising compliance with the provisions protecting private life; handling claims, reports and complaints lodged by citizens; banning or blocking processing operations that are liable to cause serious harm to individuals; checking, also on citizens' behalf, into the processing operations performed by police and intelligence services; carrying out on-the-spot inspections to also access databases directly; reporting to judicial authorities on serious infringements; raising public awareness of privacy legislation; fostering the adoption of codes of practice for various industry sectors; granting general authorizations to enable the processing of certain data categories; and participating in Community and international activities, with particular regard to the work of joint supervisory authorities as per the relevant international conventions (Schengen, Europol, Customs Information System). This Authority draws Parliament's and the Government's attention to the need for regulatory measures in the data protection sector and render mandatory opinions on regulatory instruments and administrative measures drafted by public administrative bodies. It submits an annual report to Parliament describing its activities.

Since its inception in 1997, this Authority has been active in the social, economic, political, and cultural life of the country. Special importance should be attached to the provisions made in respect of health-care, employment, banking, insurance, journalism, telecommunications, video surveillance, marketing, and public administrative agencies.

* This Authority has encouraged the adoption of a Code of practice for journalists (1998) as well as of the codes of practice related to processing of personal data for historical research purposes (2001), for statistical purposes within the framework of the National Statistics System (2002), for statistical purposes by universities, research organizations, and scientific societies (2004), and for the purposes of credit bureaus / CRAs  (2004). The use of genetic data for health care and research purposes was also regulated via an instrument (general authorization) issued in 2007.

The Authority’s website ([**www.gpdp.it**](http://www.gpdp.it/)) contains a full range of information on the decisions and opinions issued by the Authority itself along with the relevant primary and secondary legislation (in English), as follows:

Legislation on data protection and relevant issue is available at the following link: <http://www.garanteprivacy.it/web/guest/home_en/italian-legislation>

In terms of main decisions, please refer to the following link: <http://www.garanteprivacy.it/web/guest/home_en/main-decisions>

Relevant press releases are available at the following link: http://www.garanteprivacy.it/web/guest/home\_en/press-releases

Publications, including one of relevance for the study under reference is available at the following link: http://www.garanteprivacy.it/web/guest/home\_en/vademecum

**ANNEX**

(Excerpt from the DPA’s website)

More specifically, in terms of relevant legislation, mention has to be made of the following:

**Introduction**

Italy's consolidated data protection code came into force on 1 January 2004.The Code brings together all the various laws, codes and regulations relating to data protection since 1996. In particular, it supersedes the Data Protection Act 1996 (no. 675/1996), which had come into effect in May 1997. There are three key guiding principles behind the code, which are outlined in section 2:

1. Simplification;

2. Harmonisation;

3. Effectiveness.

The code is divided into three parts.

The first part sets out the general data protection principles that apply to all organizations. Part two of the code provides additional measures that will need to be undertaken by organizations in certain areas, for example, healthcare, telecommunications, banking and finance, or human resources. Part three relates to sanctions and remedies. It is expected that the second part of the code will be developed further through the introduction of sectoral codes of practice.

**Scope of the Italian data protection code** - The code applies to all processing within the State and its territories. It will also affect outside organizations that make use of equipment located within Italy, which could include e.g. PCs and other computer-based systems (see Section 5 of the Code). If an organization outside the EU is processing data on Italian territory, it must appoint a representative in Italy for the application of Italian rules (this will be necessary for notifying with the Garante, if notification is due, and providing data subjects with information notices).

**Main Features of the Data Protection Code**

**Notification** - One of the key targets for simplification was the notification process, which was made more straightforward compared to the 1996 Act in line with the EU Data Protection Directive - which allows the notification process to be simplified in cases where data processing does not adversely affect the rights and freedoms of data subjects (see Article 18(2) of the directive). Under the Italian code, organizations are only required to notify the Garante when processing higher-risk categories of data. These include, in particular, genetic and biometric data, data processed for the purpose of analyzing or profiling individuals, and credit-related information (see Section 37 of the code for additional details). This approach is also aimed at making the process more transparent and understandable for individuals.

**Data minimization** - Section 3 of the code introduces the element of data minimization into Italian data protection. The code encourages organizations to make use of non-personal data whenever possible.

**Data subjects' rights/Decision taking**- The code aims to strengthen individuals' data protection rights, allowing them to exercise their rights and instigate proceedings more easily. In an effort to simplify the complaints process, the Garante has published a complaints form on its website. The Garante 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. The turnaround for dealing with complaints has been raised to 60 days (previously it was 30 days); this period was found to be suitable in order for the Garante to work effectively and the parties to prepare their pleadings appropriately.

**International Data Transfers** - The data protection Code has incorporated and, to some extent, updated the previous rules on data transfers (data transfers are addressed in Sections 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 (see the Notification section). Additionally, the new system does not require organizations to resubmit notifications each year The rules for legitimizing transfers to non-EU countries can be found in Section 43 of the Code and include consent, meeting contractual obligations, public interest requirements, safeguarding life/health, investigations by defense counsel, use of publicly available data, processing for statistical/historical purposes. Additional provisions for legitimizing transfers are laid out in Section 44 of the Code and include transfers to countries deemed adequate by the European Commission, the adoption of contractual safeguards, and the use of binding corporate rules. Data subjects are entitled to lodge claims in Italy for non-compliance with the said contractual/corporate safeguards.

**Main Features in Respect of Specific Processing Operations**

**Human Resources Data** - The code has fully implemented Article 8 (b) of the EU directive which applies to the processing of data. Organizations 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 Section 26 of the code. For example, Section 26 (4d) allows the processing of sensitive data without consent if necessary to meet obligations under employment law.

**Health data** - Processing is allowed with the data subject's consent (which must be provided in writing) and the Garante's authorisation if the data controller is a private body. As for public bodies, processing is allowed if it is provided for in laws/regulations; however, the latter must set out the specific processing operations and purposes in detail, otherwise the relevant public bodies must specify them via ad-hoc regulatory instruments. The data subject's consent is not required, in principle, whilst the Garante's authorisation is necessary except for the processing by health care professionals that is indispensable with a view to the data subject's health and/or bodily integrity. The Garante's authorisation has been granted in the form of an instrument applying to several entities and/or processing operations, i.e. as a "General Authorisation for the Processing of Sensitive Data" by various categories of data controller (see Legislation section). It should be recalled that specific provisions are laid down in the DP Code to regulate the processing of medical data in the health care sector (Sections 75-94). In particular, health care professionals and public health care bodies may process medical data (the Code refers to "data suitable for disclosing health") with the data subject's consent and without the Garante's authorization if the processing concerns data and operations that are indispensable with a view to the data subject's health and/or bodily integrity; conversely, they may process medical data without the data subject's consent but with the Garante's authorization if the processing is indispensable to safeguard public health.

**Electronic Communications Data** - The Code has implemented the provisions contained in the E-Communications privacy directive 2002/58/EC as well as in the data retention directive (2006/24/EC) (see Title 10, Part 2 of the Code). One of the main principles is on electronic marketing which requires organizations to obtain prior consent before sending electronic marketing to consumers (see Section 130). This applies to all forms of e-marketing, including e-mail, fax, SMS/MMS etc.. Specific provisions were added to regulate telemarketing. There is also a ban on sending e-marketing from anonymous addresses - this is a breach of the data protection code as the data controller has withheld its identity. As for data retention, communications service providers (CSPs) are permitted to retain traffic data for only a six-month period in order to deal with disputes over billing and subscriber services (section 123(2) ). CSPs are also required to retain traffic data for longer in connection with law enforcement purposes; the retention periods are currently set at twenty-four months (telephone traffic data) and twelve months (electronic communications traffic data), irrespective of the given offence at issue (in pursuance of directive 2006/24/EC) (see section 132). Following ratification of Council of Europe's Cybercrime Convention (via Act no. 48/2008, which amended Section 132 of the DP Code), police authorities were enabled, under specific circumstances, to order IT and/or Internet service providers and operators to retain and protect Internet traffic data - except for contents data- for no longer than ninety days, in order to carry out pre-trial investigations or else with a view to the detection and suppression of specific offences. The order issued by police authorities must be notified to and validated by the competent public prosecutor.

**Main Features as to Compliance and Enforcement**

**Complaints** - Data subjects can settle disputes either through the courts or by lodging a complaint with the Garante in case they have been prevented from exercising access/erasure/rectification/updating rights (as per Section 7 of the code).Organisations have 30 15 days to respond and can appeal to the Garante for more time. The Garante will then have 60 days to consider the request (see above "Data Subjects' Rights/Decision Taking").

**Inspections** - The Garante's inspection powers are laid out in Section 158 of the code. When investigating organisations, the Garante can request information and documents, although these requests are not legally binding. However, if there is no cooperation, and the organisations refuses access to its systems, the Garante can apply for a judicial order to carry out an investigation.

When carrying out formal inspections, the Garante can demand copies of manual records and databases, which may be passed onto the judicial authorities. A report of the outcome is then published.

**Codes of Conduct**

**Introduction**

Legislative decree 196/2003 has enhanced the importance of codes of conduct and professional practice in respect of the protection of personal data. In particular, it provides for their adoption in several, highly significant sectors such as processing of data via the Internet and/or in the employment context, for purposes of direct marketing, by private credit reference agencies, or in connection with video surveillance activities. The main principle in this connection is that compliance with the provisions set forth in the relevant code of conduct is a prerequisite for the processing operations to be lawful - see section 12(3). Adoption of the codes of conduct takes place following the impulse given by the Italian DPA with the involvement of the relevant industry sector; a specific procedure is envisaged and the final instrument is to be published in Italy's Official Journal (the official collection of legal and regulatory instruments). This section contains the codes adopted so far in the various sectors and will be updated as appropriate.

[**- Code of Practice Applying to the Processing of Personal Data Performed with a View to Defence Investigations**](http://www.garanteprivacy.it/garante/doc.jsp?ID=1569165)

[**- Code of conduct and professional practice applying to information systems managed by private entities with regard to consumer credit, reliability, and timeliness of payments**](http://www.garanteprivacy.it/garante/doc.jsp?ID=1079077)

[**- Code of conduct and professional practice applying to processing of personal data for statistical and scientific purposes**](http://www.garanteprivacy.it/garante/doc.jsp?ID=1115480)

[**- Code of conduct and professional practice applying to the processing of personal data for statistical and scientific research purposes within the framework of the national statistical system**](http://www.garanteprivacy.it/garante/doc.jsp?ID=1565879)

[**- Code of conduct and professional practice Regarding the processing of personal data For historical purposes**](http://www.garanteprivacy.it/garante/doc.jsp?ID=1565819)

[**- Code of Practice Concerning the Processing of Personal Data in the Exercise of Journalistic Activities**](http://www.garanteprivacy.it/garante/doc.jsp?ID=1565746)

[**- Code of Ethics and Conduct in Processing Personal Data for Business Information Purposes**](http://www.garanteprivacy.it/garante/doc.jsp?ID=5483022)

**General Authorisations Issued for the Processing of Sensitive Data (as currently in force)**

**Introduction**

An authorisation by the Italian DPA is required to enable private bodies to process sensitive data (see Section 26 of the DP Code). Additional safeguards apply to the processing of judicial data. To prevent private-sector data controllers from having to apply for ad-hoc authorisations, the DP Code provides (Section 40) that "general authorisations" may also be issued by the Italian DPA. Such general authorisations may be targeted to industry sectors (e.g. banking and insurance companies) and/or specific categories of data (e.g. genetic data or medical data).Where a data controller complies in full with the provisions made in the relevant general authorisation, no ad-hoc authorisation will be required. If this were not the case, a specific application will have to be lodged with the Italian DPA; the DPA will then consider all the circumstances of the case and decide whether the authorisation is to be granted. The general authorisations currently in force for the processing of sensitive data expire on 31 december 2013.

[**- Authorisation No. 1/2014 Concerning Processing of Sensitive Data in the Employment Context**](http://www.garanteprivacy.it/garante/doc.jsp?ID=3800330)

[**- Authorisation No. 2/2014 Concerning Processing of Data Suitable for Disclosing Health or Sex Life**](http://www.garanteprivacy.it/garante/doc.jsp?ID=3800455)

[**- Authorisation No. 3/2014 Concerning - Processing of Sensitive Data by Associations and Foundations**](http://www.garanteprivacy.it/garante/doc.jsp?ID=3800792)

[**- Authorisation No. 4/2014 Concerning - Processing of Sensitive Data by Self-Employed Professionals**](http://www.garanteprivacy.it/garante/doc.jsp?ID=3810283)

[**- Authorisation No. 5/2014 Concerning - Processing of Sensitive Data by Various Categories of Data Controller**](http://www.garanteprivacy.it/garante/doc.jsp?ID=3017707)

[**- Authorisation No. 6/2014 Concerning Processing of Sensitive Data by Private Detectives**](http://www.garanteprivacy.it/garante/doc.jsp?ID=3816659)

**[- Authorisation No. 7/2014 Concerning Processing of Judicial Data by Private Entities, Profit-Seeking Public Bodies and Public Entities](http://www.garanteprivacy.it/garante/doc.jsp?ID=3826271)**

**[- Authorisation No. 8/2014 for the Processing of Genetic Data](http://www.garanteprivacy.it/garante/doc.jsp?ID=3831387)**

* **[Authorisation no. 9/2014 - General Authorisation to Process Personal Data for Scientific Research Purposes](http://www.garanteprivacy.it/garante/doc.jsp?ID=3786078)**

In terms of main decisions, mention has to be made of the following:

A selection of the main decisions by the Italian Data Protection Authority, arranged by subject and by date, and expanded continuously:

**Banking and Financial Sector**

* [Data Sharing and Tracking of Transactions in the Banking Sector - 12 may 2011](http://www.garanteprivacy.it/garante/doc.jsp?ID=1868766)
* [Provisions Applying to Corporate Mergers and Split-Ups - 9 may 2009](http://www.garanteprivacy.it/garante/doc.jsp?ID=1625292)
* [Guidelines for the Processing of Customers' Data in the Banking Sector - 25 october 2007](http://www.garanteprivacy.it/garante/doc.jsp?ID=1478096)

**Biometrics & Genetic Data**

* [General Application Order Concerning Biometrics - 12 november 2014](http://www.garanteprivacy.it/garante/doc.jsp?ID=3590114)
* [General Authorisation for the Processing of Genetic Data - 13 december 2012](http://www.garanteprivacy.it/garante/doc.jsp?ID=2474250)
* [Limitations Applying to the Taking of Fingerprints and Image Acquisition by Banks - 27 october 2005](http://www.garanteprivacy.it/garante/doc.jsp?ID=1671299)
* [Access to Restricted Areas and Biometrics - For A Proportionate Use of Fingerprints - 23 november 2005](http://www.garanteprivacy.it/garante/doc.jsp?ID=1166892)
* [Use of Fingerprints for Assiduity Control at the Workplace (Prior Checking) - 21 july 2005](http://www.garanteprivacy.it/garante/doc.jsp?ID=1166892)

**Business Information**

* [Business Information: Only Relevant Data May Be Processed - 30 october 2008](http://www.garanteprivacy.it/garante/doc.jsp?ID=1589979)

**Business Sector**

* [Practical Guidelines and Simplifying Measures for SMEs - 24 may 2007](http://www.garanteprivacy.it/garante/doc.jsp?ID=1435985)

**Clinical Drug Trials**

* [Guidelines for Data Processing within the Framework of Clinical Drug Trials (revised) - 14 august 2008](http://www.garanteprivacy.it/garante/doc.jsp?ID=1544272)

**Credit Reporting**

* [Balancing of Interests: Data Collection by CRAs without Consents - 14 november 2004](http://www.garanteprivacy.it/garante/doc.jsp?ID=1671380)

**Data Retention**

* [Secure Retention of Telephone and Internet Traffic Data - 24 july 2008](http://www.garanteprivacy.it/garante/doc.jsp?ID=1542849)
* [Security in Internet and Telephone Traffic Data - 17 january 2008](http://www.garanteprivacy.it/garante/doc.jsp?ID=1502599)

**Debt Collection**

* [Debt Collection and Processing of Personal Data - 30 november 2005](http://www.garanteprivacy.it/garante/doc.jsp?ID=1296710)

**Electoral Propaganda**

* [Electoral Propaganda: A Decalogue by the Garante - 7 september 2005](http://www.garanteprivacy.it/garante/doc.jsp?ID=1187710)

**Electronic Communications, Internet**

* [Simplified Arrangements to Provide Information and Obtain Consent Regarding Cookies - 8 may 2014](http://www.garanteprivacy.it/garante/doc.jsp?ID=3167654)
* [Injunction and Order Issued Against Google Inc. - 18 December 2013](http://www.garanteprivacy.it/garante/doc.jsp?ID=3133945)
* [Ordering Google Inc. to block data processing in connection with the "capturing" of communications on Wi-Fi networks and lodging a report with judicial authorities - 9 september 2010](http://www.garanteprivacy.it/garante/doc.jsp?ID=1750713)
* [MMS and Data Protection - 12 march 2003](http://www.garanteprivacy.it/garante/doc.jsp?ID=1589979)
* [Social Networks - Watch Out for Side Effects - 30 october 2008](http://www.garanteprivacy.it/garante/doc.jsp?ID=1303462)
* [Enhanced Security Measures in Processing Telephone Traffic Data - 1 june 2006](http://www.garanteprivacy.it/garante/doc.jsp?ID=1303462)

**Employment**

* [Vehicle Geo-Location and Employer-Employee Relations - 4 October 2011](javascript:void(0)/*332*/)
* [Guiding Principles on the Processing of Employees' Personal Data in the Public Sector - 14 june 2007](http://www.garanteprivacy.it/garante/doc.jsp?ID=1693793)
* [Guidelines Applying to the Use of E-Mails and the Internet in the Employment Context - 1 march 2007](http://www.garanteprivacy.it/garante/doc.jsp?ID=1427027)
* [Guidelines on DP and Employment in the Private Sector - 23 november 2006](http://www.garanteprivacy.it/garante/doc.jsp?ID=1427027)

**Geo-Location**

* [Vehicle Geo-Location and Employer-Employee Relations - 4 October 2011](http://www.garanteprivacy.it/garante/doc.jsp?ID=2444921)

**Health Data**

* [Guidelines on processing personal data for dissemination and publication on exclusively health-related web sites - 25 january 2011](http://www.garanteprivacy.it/garante/doc.jsp?ID=1683328)
* [Guidelines on Online Examination Records - 25 june 2009](http://www.garanteprivacy.it/garante/doc.jsp?ID=1634292)
* [Guidelines on the Electronic Health Record and the Health File - 16 july 2009](http://www.garanteprivacy.it/garante/doc.jsp?ID=1672821)

**Household and Social Activities**

* [Data Protection and Management of Condos - 18 may 2006](http://www.garanteprivacy.it/garante/doc.jsp?ID=1589979)

**New Media**

* [Guidelines on processing personal data for dissemination and publication on exclusively health-related web sites - 25 gennaio 2012](http://www.garanteprivacy.it/garante/doc.jsp?ID=1879894)
* [Interactive TV: Compliance with DP Legislation - 3 february 2005](http://www.garanteprivacy.it/garante/doc.jsp?ID=1116787)

**Marketing**

* [Guidelines on Processing Personal Data to Perform Customer Satisfaction Surveys in the Health Care Sector](http://www.garanteprivacy.it/garante/doc.jsp?ID=3853781)
* [Loyalty Cards and Programmes: Guidelines - 24 february 2005](http://www.garanteprivacy.it/garante/doc.jsp?ID=1109624)

**Media**

* [Publishing Transcripts of Tapping Records - 21 june 2006](http://www.garanteprivacy.it/garante/doc.jsp?ID=1301195)

**New Technologies**

* [*"Smart" (RFID) Tags: Safeguards Applying to Their Use - 9 march 2005*](http://www.garanteprivacy.it/garante/doc.jsp?ID=1121107)

**Notification of Processing Operations**

* [Simplification of Notification Requirements and Forms - 9 december 2008](http://www.garanteprivacy.it/garante/doc.jsp?ID=1630455)
* [Provision by the italiana Data Protection Authority - Cases exempted from notification - 31 march 2004](http://www.garanteprivacy.it/garante/doc.jsp?ID=1672979)

**Public Administration**

* [Guidelines for the Processing by Public Bodies in Connection with Web-Based Communication and Dissemination - 19 march 2011](http://www.garanteprivacy.it/garante/doc.jsp?ID=1803707)

**Security Measures**

* [Implementing Measures with Regard to the Notification of Personal Data Breaches – 4 April 2013](http://www.garanteprivacy.it/garante/doc.jsp?ID=2414592)
* [Measures and arrangements applying to the controllers of processing operations performed with the help of electronic tools in view of committing the task of system administrator - 27 november 2008](http://www.garanteprivacy.it/garante/doc.jsp?ID=1628774)
* [Simplifying the Security Measures Set Forth in the Technical Specifications Contained in Annex B to the Data Protection Code - 27 november 2008](http://www.garanteprivacy.it/garante/doc.jsp?ID=1583482)
* [Electrical and Electronic Waste and Data Protection - 9 december 2008](http://www.garanteprivacy.it/garante/doc.jsp?ID=1583482)

**Spam**

* [Spamming: Guidelines by the Italian DPA - 29 may 2003](http://www.garanteprivacy.it/garante/doc.jsp?ID=1589969)

**Tax Returns**

* [Taxpayers' Lists on the Internet - 6 may 2008](http://www.garanteprivacy.it/garante/doc.jsp?ID=1519208)

**Telephony & Telemarketing**

* [**General Injunction Regarding the So-Called "Silent Calls"** - 20 February 2014](http://www.garanteprivacy.it/garante/doc.jsp?ID=3318874)
* [Requirements Applying to the Processing of Personal Data for Marketing Purposes as Performed by Relying on Operator-Assisted Telephone Calls, Following the Creation of the Public Opt-Out Register - 19 January 2011](http://www.garanteprivacy.it/garante/doc.jsp?ID=1791330)
* [Profiling and Electronic Communications - 25 june 2009](http://www.garanteprivacy.it/garante/doc.jsp?ID=1636001)
* [Measures Imposed on the Controllers of Databases Set up from Telephone Subscriber Directories Compiled Prior to 1 August 2005 Following the Derogations Introduced by Section 44 of Decree no. 207/2008 - 12 March 2009](http://www.garanteprivacy.it/garante/doc.jsp?ID=1613568)
* [Measures Concerning Itemised Billing - 13 march 2008](http://www.garanteprivacy.it/garante/doc.jsp?ID=1522362)
* [Unsolicited Telephone Services - 16 february 2006](http://www.garanteprivacy.it/garante/doc.jsp?ID=1290823)
* [Access to Telephone Data: Safeguards Applying to Incoming Calls - 3 november 2005](http://www.garanteprivacy.it/garante/doc.jsp?ID=1299003)

**Video Surveillance**

* [Video Surveillance - Guidelines by the Italian DPA - 8 april 2010](http://www.garanteprivacy.it/garante/doc.jsp?ID=1734653)

(http://www.garanteprivacy.it/web/guest/home\_en/main-decisions)

More specifically, as a way of examples, mention can be made of relevant press releases (<http://www.garanteprivacy.it/web/guest/home_en/italian-legislation>):

*Google to comply with the privacy measures set forth by the Italian DPA Verification protocol approved by the DPA Google will implement all the measures imposed by the Italian DPA to protect Italian users' privacy. For the first time in Europe, it will be the subject of regular checks to monitor progress status of the actions to bring its platform into line with domestic legislation. The Italian DPA approved the verification protocol referred to in its order of July 2014 to Mountain View. This marks a shift from the laying down of measures by the DPA to the practical implementation of such measures by Google, which will have to be fully compliant by 15 January 2016. The protocol envisages quarterly updates on progress status and empowers the DPA to carry out on-the-spot checks at Google's US headquarters to verify whether the measures being implemented are in compliance with Italian law. The protocol enables the DPA to continuously monitor the changes Google is required to make to the processing of personal data relating to users of its services – including its search engine, emailing, YouTube and social networking services. The key measures Google is to implement in the course of 2015 are summarized below: Privacy Notice Google will have to improve its privacy policy by making it unambiguous and easily accessible and tailoring it to the specific service (such as Gmail, Google Wallet, Chrome, etc. ). The notice will have to detail purposes and mechanisms of the processing of users' data including profiling as performed by combining data across multiple services, the use of cookies and other identifiers such as fingerprinting – that is, the collection of information on the use of terminal equipment or devices by users and the storage of this information directly in the company's servers. Google will have to set up an archive including previous versions of its privacy notices to allow users to keep track of the changes made over time. Consent In order to profile users of its services, Google will have to first obtain their informed consent. This requirement will have to be implemented, though via different mechanisms, both for new accounts and for existing Google accounts. Google will also have to fully implement the measures set forth in the decision adopted by the Italian DPA in May 2014 regarding use of cookies and other identifiers – including unregistered users. All data subjects will have to be afforded in any case the right to object to the processing of their data for profiling purposes. Data Storage and Deletion The US giant will have to further improve its data storage and deletion mechanisms as for users' personal information. In particular, a specific timeframe will have to be in place regarding data deletion from both online and back-up systems. Internal rules on anonymization will have to be revised to ensure that the relevant procedures are fully effective and compliant with the guidance already provided by European DPAs. Users' Requests for Delisting Search Results An exchange of information will continue regarding delisting requests received by Google from Italian users so as to monitor the implementing arrangements of the so-called right to be forgotten. Rome, 20 February 2015*

*MORE SAFEGUARDS FOR GOOGLE USERS IN ITALY: THE ITALIAN GARANTE DRAWS THE LINE*

*Mountain View will have to improve transparency in processing data and provide more safeguards to users*

*Users of Googles services (including Search) in Italy will be better protected. The Italian Garante has ruled that the IT giant from Mountain View may not use users data for profiling without their prior consent; furthermore, Google will have to inform users specifically that it is profiling them for marketing purposes.*

*This****[decision](http://www.garanteprivacy.it/garante/doc.jsp?ID=3295641)****and the measures it provides for concluded the proceeding the Italian Garante had started last year following the changes made by Google to its privacy policy worldwide. This is the first decision in Europe that – as part of a coordinated action with other European DPAs and following the  judgment by the Court of Justice of the EU on the right to be forgotten – does not limit itself to urging Google to comply with privacy legislation as it actually lays down specific measures Google must take to achieve full compliance with the law. Google has merged the individual data management rules into a single document, which relates to the many features it offers: from Gmail to social networking (Google Plus); from online payments (Google Wallet) to video sharing (YouTube); from online mapping (Street View) to statistical analysis (Google Analytics). Thus, Google has made the individual features integrated and interoperable and matches and combines the data coming from users interaction with multiple services.  
In the course of the proceeding, which also included several hearings with the companys representatives, Google did take measures to bring its privacy policy more into line with the applicable legislation. Nevertheless, the Garante found that several criticalities remained concerning the inadequate information provided to users, the failure to request users consent for profiling purposes, and the unspecified data retention periods; accordingly, the Garante laid down a set of measures applying to all the services offered by Google.*

*Information to Users*

*The Garante required Google to implement a multi-layered information system so as to provide the most relevant information via a first-layer notice mentioning what data are being processed (device location data, IP-addresses, etc.), where users may apply (in Italian) to exercise their rights, and so on. A second-layer notice will include more detailed, specific information on the individual services.*

*More importantly, Google will have to clearly explain – in the first-layer notice – that users personal data are being monitored and used, among other things, to profile them for delivering targeted ads, and that users data are also collected via more sophisticated techniques than cookies (e.g., fingerprinting). The latter is a system whereby information on the use of a device is collected and stored directly in the companys servers – whilst cookies are installed, for instance, in the users PC or smartphone.*

*Consent  
Google will have to obtain users prior consent in order to use their data (whether coming from the use of emailing services or collected by matching and combining information from different services or else by way of cookies and fingerprinting) for the purposes of profiling and delivering targeted behavioral ads. This means that Google may no longer regard the mere fact of using one of its services as unconditional acceptance of rules that have not left – so far – any room for decision-making by data subjects on how their personal data ought to be processed.  In this connection, the Garante also proposed an innovative, user-friendly mechanism that does not affect user experience substantially and enables users to make affirmative, informed choices on whether to consent or not to consent to profiling also with regard to the individual services being used.*  
*Data Retention*

*Google will have to set specific retention periods based on the provisions contained in the Italian data protection Code. This applies both to the data stored in the so-called active systems and to the data that is stored subsequently in back-up systems. As for the deletion of personal data, the Garante required Google to comply with deletion requests made by Google account holders (who therefore can be identified easily) within two months (for data stored in active systems) or else within six months (for data stored in back-up systems). However, the Garante considered it appropriate to await developments related to implementation of the CJEUs judgment on the right to be forgotten as for deletion requests concerning use of Googles search engine*. *Google will have to comply with the measures laid down by the Garante in eighteen months. Meanwhile, the Garante will monitor implementation of those measures and the company will have to submit – by 30 September 2014 – a verification protocol which, once undersigned, will become binding. This protocol will regulate timeline and mechanisms for the supervision to be performed by the Garante on Googles activities.* *Rome, 21 July 2014*

*Social Privacy: How to Protect Yourselves in the Age of Social Networks  
New guidance by the Italian DPA to avoid the pitfalls of social networking*

*Young people expose their most intimate secrets and post pictures to tease one another or capture someone's love; parents often do not know where to start with the Web; users may install the wrong app lured by the fact that it is ‘for free'; acclaimed professionals endanger their professional contacts; harassers and cyber-bullies take advantage of their (supposed) anonymity to go for the helpless.*

*These are but a few of the issues tackled by the Italian Garante (data protection authority) in its guidance called ‘Social Privacy: How to Protect Yourselves in the Age of Social Networks' (web document No.****[3922719](http://www.garanteprivacy.it/garante/doc.jsp?ID=3922719)****). The guidance provides an analysis of the main issues, problems and opportunities related to social networks along with tips and solutions that can be helpful to the ‘2.0 generation' – inexperienced users, teachers, families, experts, managers.*

*The Vademecum takes stock of the new frontier opened up not only by conventional social networks, but also by the many instant messaging platforms that have sprouted up as quickly as smartphones, tablets and phablets have become commonplace – including the so-called ‘wearable technology' such as ‘smart' watches or glasses.*

*To raise user awareness and provide additional food for thought along with effective safeguards, the DPA is proposing a Decalogue where the opportunities made available by digital technologies are described and advice is given on how to avoid possible pitfalls. Special attention is paid to identity theft, sexting and cyberbullying, which can ruin the lives of young people (and especially children) for real.*

*‘There is no barrier any longer' pointed out the President of the DPA, Antonello Soro, ‘between digital life and real life. What happens online is increasingly impacting the offline world – our daily lives and personal relationships. This is why one should never lose sight on the Internet of the need for a balanced relationship between new social communication channels and the protection of your own and others' dignity.'*

*Google pays 1-million-Euro fine imposed by the Italian DPA because of Google's Street View service*

*Google paid a 1-million-Euro fine imposed by the Italian DPA because of Google's Street View service. The facts at issue date back to 2010, when the "Google cars" were driving throughout Italy without being recognizable as such so that whoever did not want to be "captured" in the images taken by the "Google cars" could not decide in advance what to do. Several complaints had been lodged on this ground with the Italian DPA against the pictures posted online – which actually are stored for long and may be zoomed into.*

*A decision by the Italian DPA (see web doc. No.****[1759972](http://www.garanteprivacy.it/garante/doc,jsp?ID=3133945)****) had ordered Google to make the "Google cars" easily identifiable by way of visible notices or stickers and publish the list of the locations to be visited by the Google cars three days beforehand, by also specifying the neighbourhoods or areas visited in large cities. Google was also required to publish similar notices on the local news sections of at least two dailies and to broadcast this information via a local radio station in each of the Regions to be visited. These measures were implemented timely by Google.*

*Having concluded the proceeding aimed at the possible imposition of penalties, the Italian DPA decided to impose a fine amounting to 1 million Euro (which was paid by Google a few weeks ago) (see web doc. No.****[2954309](http://www.garanteprivacy.it/gartante/doc.jsp?ID=2954309)****); this was done by having regard, in particular, to the circumstance that the unlawfully collected information would be pooled into a large database of substantial import – i.e. the one set up by Google in connection with the Street View service.*

*The Italian DPA decided to rely on the provision in the Privacy Code that is aimed at ensuring effective sanctions are imposed on major business entities - exactly by considering that Google's consolidated turnover for 2012 totalled over 50 billion dollars.*

*Rome, 3 April 2014*

*Google: The Italian Dpa Initiates a Proceeding to Establish Compliance with Italian Legislation  
A Coordinated Action with the DPAs from 5 EU Member States*

*The Italian DPA initiated a proceeding in respect of Google Inc. to establish compliance with the Italian legislation on the protection of personal data. The focus is on whether the processing of personal data by the Mountain View company is in line with the principles of relevance, non-excessiveness and data minimization as well as with the obligations concerning users' information and consent.*

*This proceeding is part of a joint action undertaken by an ad-hoc task force that includes the DPAs from France, Germany, Italy, Netherlands, Spain and the United Kingdom.*

*The Working Party made up of all the DPAs from the 27 EU Member States analysed Google's privacy policy between March and October 2012 to check whether it was in line with the European data protection directive (95/46/EC). The new privacy policy allows Google, among other things, to combine data from users of different services – from Gmail to YouTube and Google Maps, to name but a few of them –  without any limitations.*

*The findings of this analysis were published on 26 October 2012 and the EU DPAs urged Google Inc. accordingly to make several changes within 4 months as those changes were considered necessary to bring the processing operations into line with the legislation in force.*

*After the 4-month period expired, representatives from Google Inc. asked for a meeting with the Task Force; the meeting was held on 19 March 2013  but no steps have been taken so far to implement the changes although the company had stated their willingness to do so.  
Thus, each of the six DPAs involved will carry out additional inquiries by officially initiating separate proceedings, which will nevertheless be simultaneous as well as coordinated very closely.*

*"Google may not collect and process personal data from European citizens without taking account that specific rules are in place in the EU to protect citizens' fundamental rights. The joint action by European DPAs is meant to reaffirm this principle and ensure that those rights are safeguarded" – stated the Italian DPA's President, Mr. Antonello Soro. "The Italian DPA has long been working on the international level exactly to make sure that EU citizens' privacy is respected not only by EU undertakings, but also by Internet giants and all electronic communications companies regardless of where they are established. We want to prevent "safe havens" from being set up where fundamental rights are not upheld", Mr. Soro concluded.*

*Rome, 2 April 2013*

*Public Administration on the Internet: The Rules to Respect Citizens' and Employees' Privacy*

*Only indispensable information should be posted online, and it should remain online for the appropriate periods, whilst technological measures must be in place to prevent file manipulation and bulk duplication and special care is required in allowing external search engines to retrieve the data posted on an institutional website.*

*The Italian data protection authority laid down the****[rules](http://www.garanteprivacy.it/garante/doc.jsp?ID=1803707" \t "_blank)****to be complied with by public administrative bodies when posting administrative records and documents that contain personal data, so as to not to violate citizens' and employees' privacy and respect the principles set forth in the relevant legislation.*

*The Guidelines issued by the Italian DPA make up an initial set of measures and arrangements public administrative bodies are required to implement regardless of the purposes for which the information is posted online (transparency, publicity, access).*

*The Guidelines are the outcome of a complex preparatory activity and take also account of the considerations submitted by various public bodies, local authorities, and consumer associations as part of the public consultation launched by the DPA a few months ago.*

*The main points made in the Guidelines can be summarized as follows:*

*- Public administrative bodies may only post records/documents containing personal data online if this is provided for in laws and/or regulations; they must comply with data minimization, proportionality, and data relevance principles, whilst the ban on disseminating health-related data is left unprejudiced.*

*- The appropriate technological measures should be taken to prevent the online information from being erased, changed and/or extrapolated.*

*- The records/documents should be retrieved, if possible, by way of internal search engines, whilst the indexing of such records/documents by external search engines should be limited. Relying on internal search engines can ensure that access will be consistent with the purposes for which the information was disclosed as well as preventing the data from being tampered with and/or taken out of their context – i.e. this will prevent arbitrary extrapolation of the information along with the resulting impossibility to control their use.*

*- The data must remain available for no longer than is necessary in pursuance of the sector-related legislation. Failing such legislation, each public administrative body should determine the appropriate deadlines for removal of the posted data.*

*- Finally, alert systems and software should be deployed to prevent reproduction and re-use of the files containing personal data; such systems can detect and report any dubious  access so as to take the adequate countermeasures.*

*Rome, 4 April 2011*

*Captured" Communications on Wi-Fi Networks: The Italian DPA Requires Google to Block Data Processing and Reports the Case to Judicial Authorities*

*The Italian DPA ordered Google to block the processing of "payload data" captured by Google StreetView cars and reported the case to judicial authorities that should establish whether the data collection entailed any criminal offences.*

*The DPA had started investigating the case in May this year; it had been informed that the Google cars driving throughout Italy had not only collected pictures, but also "captured" fragments of electronic communications ("payload data") from April 2008 via specific software, if those communications were transmitted between users that relied on non-secured Wi-Fi networks.*

*Google provided the information requested by the DPA and confirmed that payload data had actually been captured by its cars; however, it specified that the information had been collected mistakenly and was so fragmented that it could not be considered to amount to personal information. The company stated that this information was stored in servers located in the USA and had never been used or disclosed to third parties.*

*Conversely, the DPA holds the view that the data collection in question does entail the factual risk that some of the captured information is personal data (i.e. that it can be related to identified or identifiable individuals) – considering that the data were collected systematically and over a long time span (until May 2010). Accordingly, Google might be seriously in breach of criminal law as it has not only violated the Data Protection Code, but also possibly infringed some provisions contained in Italy's Criminal Code – such as those banning illicit interception of communications that take place over an IT or computerised system (section 617-quater) and the installation (in breach of the law) of "equipment that is suitable for intercepting, preventing or discontinuing" communications of the same type (section 617-quinquies).*

*For the above reasons, the DPA decided to report the case to judicial authorities, which should now establish whether criminal offences have been committed. Since the payload data may serve as proof of such criminal offences, if any, the DPA decided additionally they should not be deleted from the servers where they are currently stored and ordered their processing to be blocked – whereby Google was required to discontinue any processing operations involving them.*

*21 September 2010*

*Medical Examinations Online*

*Patients may receive blood test results, X-Rays and medical examinations directly on their PCs without having to wait in a queue at medical labs and health care agencies; however, the data subject's consent is mandatory along with the use of appropriate passwords.*

*The "****[Guidelines for Online Medical Examinations](http://www.garanteprivacy.it/garante/doc.jsp?ID=1634292)****" issued by the DPA set forth stringent measures to ensure the protection of patients' medical data when such data are sent via email and/or "downloaded" directly by patients from the websites of the health care institutions they applied to.*

*Medical reports have long been accessible in electronic format at medical labs, hospitals and nursing homes; however, no specific regulations are in place in a data protection perspective. This made it necessary for the DPA to step in – pending the enactment of appropriate legislation – so as to ensure that this important as well as innovative mechanism to provide health care in a technologically advanced manner would be implemented further in compliance with clear-cut, harmonised rules.*

*The main points made in the Guidelines are as follows:*

*- Joining the online service must be on a voluntary basis; electronic documents should not replace paper-based ones, which will have to be available in any case. Patients should only give their consent following clear-cut, detailed information including an explanation of all the features of the "online medical reporting" service.*

*- The medical report will remain available online for up to 45 days and will have to be accompanied by an evaluation written by the competent physician, who should be ready to provide additional information at the data subject's (patient's) request.*

*- In order to provide these services, public and private health care bodies will have to implement adequate technological security measures including the use of encryption standards, strong authentication systems, online validation of email addresses, and password-protected files. If they plan to also offer the option of archiving medical reports to enable their future consultation online, they will have to provide patients with an additional, specific information notice and obtain their consent separately.*

*The Guidelines take account of the considerations and comments made by public and private health care bodies and practitioners, family doctors, paediatricians, trade associations, and patients' associations.*

*21 December 2009*

For additional information please also refer to the following Authority’s publications:

http://www.garanteprivacy.it/web/guest/home\_en/vademecum

1. The constitutional court consists of fifteen judges; one-third being appointed by the Head of State, one-third by the Parliament in joint session, and one-third by ordinary and administrative Supreme Court. [↑](#footnote-ref-1)
2. https://www.agcom.it/ [↑](#footnote-ref-2)
3. Because of its particular nature, the mass media and information sector is the subject matter of a number of specific provisions in the law under reference (Article 7). These particular provisions do not replace the general rules governing any type of company, but are additional to them. [↑](#footnote-ref-3)
4. Act 112/2004 has effectively moved forward the switch from analogical to digital broadcasting, with the aim of increasing the number of TV channels (a process initiated in 2008). This has actually given greater independence and organizational autonomy to the public radio and television broadcasting service franchisee. It has placed RAI on an equal footing with all other joint stock companies, also in terms of their organization and management (Article 20 (1)). In this context, mention should be made also of the following: The start-up of terrestrial digital broadcasting as a result of Act 112/2004 has increased the number of channels free of charge by between four-fold and six-fold (as of 2014), and has consequently increased the television offering and enhanced pluralism — bringing Italy to be one of the countries with the highest number of channels ever, in the world. [↑](#footnote-ref-4)
5. [1] The complaints are mainly about audio-visual works (movies, tv series, live football games) music and pictures works, while smaller percentages are reached by editorial works, such as newspapers and journalistic contents. [↑](#footnote-ref-5)
6. Decree-Law No. 63 of 18 May 2012 (‘Decree-Law No 63/2012’) amended Article 43 of the Italian Audio-Visual Media Single Act (Law No. 177/2005) so that the scope of the overall revenue of the Integrated Communications System (SIC) includes also revenue deriving from advertising on line and on various platforms, whether or not direct, including resources obtained by search engines and social or sharing platforms. [↑](#footnote-ref-6)
7. Judgement in Case No. 1739/2018 (TAR Lazio, Roma, sez. I, sentenza del 14/02/2018 n. 1739). [↑](#footnote-ref-7)
8. The list of current members of the Technical Roundtable includes: Google Italy, Facebook Italy, Fondazione Wikimedia Italia, Federazione Italiana Editori Giornali, Confindustria Radio Televisioni, Aeranti-Corallo, Web Radio Associate, Associazione Nazionale Editoria di Settore, Associazione Nazionale Stampa Online, RAI, RTI Mediaset, La7, Sky Italia, Ciaopeople, Pagella Politica, AGI, Adnkronos, Ordine Nazionale dei Giornalisti, Federazione Nazionale della Stampa Italiana, Unione Cattolica Stampa Italia, Utenti Pubblicità Associati, Istituto dell'Autodisciplina Pubblicitaria, Unione Nazionale Imprese di Comunicazione, Associazione Aziende di Comunicazione, IAB Italia, Netcomm, Guardia di Finanza - Nucleo Speciale per la Radiodiffusione e l'Editoria, ANES. [↑](#footnote-ref-8)