Balancing the interests in the context of data retention (INVODAS)

Italia

Amedeo Arena

Part 1: General overview of the legal transposition, the national (societal) context and the constitutional/fundamental rights legal framework

A. State of play of the transposition of the Directive 2006/24/EC

I. Legal provisions

- *Introductory remark:* If national legal provisions mandating the retention of electronic communications data without any *specific* reason (i.e. stockpiling, without an actual, concrete cause) have existed already before the Directive 2006/24/EC (in the following: "the Directive") was enacted, please also make reference to these when answering to questions 5 to 35.

- *Introductory remark:* Most of the questions concerning retention obligations refer to the national provisions transposing the Directive. Some questions, however, make explicit reference to the "national law" or the "national legal system" as a whole. In these cases, we request you to provide more comprehensive information. In any case, only retention *without a specific reason* (i.e. stockpiling, without an actual, concrete cause) of data generated or processed in *electronic communications* is concerned by this questionnaire. Other retention obligations, for instance those requiring that there be a suspicion of a crime having been committed, are not covered by this questionnaire.

1. Have the provisions of the Directive already been transposed into national law?

At the legislative level, the Directive was transposed into national law by Legislative Decree no. 109/2008 ("the Transposition Decree" or "TD"), which amended some provisions of Legislative Decree no. 196/2003 "Personal Data Protection Code" ("PDPC"). In particular, the TD introduced some new definitions in addition to those already set out in Article 4 PDPC (see reply no 8) and amended the rules concerning data retention (*see* Article 132, 154 and 162-bis PDPC).

The official version (in Italian) of the TD is available at: http://www.camera.it/parlam/leggi/deleghe/testi/08109dl.htm

At the regulatory level, the *Garante per la protezione dei dati personali* (the Italian authority responsible for the protection of personal data, hereafter: the "Garante") anticipated the legislature with its Decision of 17 January 2008, setting out the technical arrangements for the protection of retained data (hereafter: the "Technical Arrangements Decision" or "TAD"). As the TD came into force, however, in order to ensure consistency of the TAD with the higher-ranking rules enacted by the legislature, the Garante adopted its Decision of 24 July 2008 introducing some (minor) amendments to TAD recitals and operative provisions. The TAD was again amended by Decision 29 April 2009, which postponed the implementation deadline for the technical requirements set out in the TAD (N.B.: references in the replies to this questionnaire to the "TAD" must be read as referring to the Decision of 17 January 2008 as subsequently amended by the two aforesaid Decisions).

- ***If transposition has not at all, or only in parts, been accomplished:***

2. **What are the reasons for the transposition not (or only in Articles) to have been effected (e.g. (purely) formal delays in the legislative procedure, constitutional law concerns, legal policy issues, socio-ethical concerns, incompatibility with the national legal system etc)?**

   /

3. **Is transposition still intended? If so: What is the current state of play of the transposition process? Until when is it likely to be finalised?**

   /

4. **In case draft legal acts are existent, or a law that had already been enacted/come into force has subsequently been abrogated by a court decision or for other reasons: Please describe the content of the provisions on the basis of questions 5, and 7 to 35.**

   /

- ***If transposition has been accomplished:***

General questions

5. **Is there an English version of the texts available? If so: Please indicate the respective URL.**

   An English language version of the PDPC (Legislative Decree no. 196/2003) as amended by the Transposition Decree is available on the Garante's website.

   (http://www.garanteprivacy.it/garante/document?ID=1219452)

   As to the TAD, no English language version of the wording currently in force is available. The Garante's website features an English version of Decision of 17 January 2008, i.e. the TAD prior to its amendment by Decision 24 July 2008 and

Decision 29 April 2009.

(http://www.garanteprivacy.it/garante/doc.jsp?ID=1502599)

6. Since when have the relevant regulations been in force? Are there any transition periods in place regarding the application of these regulations?

The Transposition Decree entered into force on July 3, 2008. The TD set out only two transitional arrangements. The first one concerned the obligation, introduced *ex novo* by the TD, to retain unsuccessful calls data for a period of 30 days (Article 132, par. 1-bis PDPC). According to Article 6, par. 3 TD, that obligation entered into force three months after the entry into force of the TD itself. The second transitional arrangement, laid down in Article 6, par. 5 TD, granted Internet Access Providers a period of 90 days from the entry into force of the decree to ensure availability and uniqueness of IP addresses.

The Technical Arrangements Decision, in its earliest version, required the implementation of a number of technical arrangements by 31 October 2008. That deadline was first extended, pursuant to the Garante's Decision of 24 July 2008, to 30 April 2009 (except for the "strong authentication" requirement for personnel accessing traffic data, whose implementation deadline was deferred until 30 June 2009). In view of the difficulties reported by providers in achieving compliance with those requirements, the Garante, in its Decision of 29 April 2009, further deferred the implementation deadline to 15 December 2009 and enjoined all the providers concerned to report to the Garante about the implementation steps undertaken.

7. What type of legal act do the existing rules meant to transpose the Directive's provisions pertain to (e.g. Act of Parliament, decree-law, regulation/decree, administrative provisions etc)? Please give an overview of all legal provisions enacted for this purpose (stating the type of legal act and the matter regulated therein) and describe

a) whether "more important" matters have been dealt with by (parliamentary-enacted) legislation whereas provisions of a more technical/technology-oriented character are tackled by decrees/administrative provisions, and

The Directive was transposed into Italian law by way of a Legislative Decree (*Decreto Legislativo*), i.e. an act adopted by the Government in accordance with the requirements and guidelines set out by the Parliament in an earlier Enabling Law (*Legge delega*). In the case of the TD, the relevant Enabling Law is Law 6 February 2007, no. 13 (Official Journal no. 40 of 17 February 2007), also known as the "EU Law 2006" (*Legge comunitaria 2006*) in that it sets out the necessary arrangements to ensure compliance with EU obligations as of 2006. Legislative Decrees, along with Laws passed by the Parliament (*Leggi ordinarie*) and emergency Decree-Laws adopted by the Government (*Decreti-legge*), rank directly below the Constitution in the internal hierarchy of legal acts.

As to the regulatory level, Article 132 PDPC, par. 5, PDPC, read in conjunction

with Article 17 PDPC, empowers the *Garante* to adopt measures and arrangements providers must comply with in the context of telephone and Internet traffic data retention. It is on the basis of this provision, that the Garante adopted *inter alia* the TAD and the amendments thereof.

Moreover, Article 3, par. 2, TD provides for that data retention obligations can be extended to new categories of data (i.e. other than those detailed in Article 3, par. 1, TD) by way of a Decree (i.e. a regulatory act) adopted either by the President of the Council of Ministers or the Minister for Innovation and Public Administration, in agreement with the Ministers for European Policies, Economic Development, Home affairs, Justice, Treasury and Defence, following consultation of the *Garante.* No such decrees have been adopted so far.

b) whether the types of legal acts chosen for the different matters regulated correspond to those usually chosen in your legal system for such kind of matters.

The Data Retention Directive transposition process is entirely consistent with the usual pattern followed by the Italian legislature in transposing other EU directives. Regrettably, the transposition deadline set out in Article 15(1) of Directive 2006/24 (i.e. 15 September 2007) was not met (the TD was adopted on 30 May 2008), albeit as per Article 15(3) of the Directive, Member States were entitled to postpone its application to the retention of communications data relating to Internet Access, Internet telephony and Internet e-mail until 15 March 2009.

Quite remarkable is instead the early directive implementation carried out by the Garante, which availed itself of its existing regulatory powers under the PDPC to bring Italian regulations in line with the directive even in the absence of legislative transposition measures (which would be adopted four months later).

8. Are the terms defined in art. 2 para. 2 of the Directive also defined within the national law transposing the Directive? If so: To what extent do the definitions given therein differ from those in art. 2 para. 2? Are there any other terms mentioned in the Directive or in the directives referred to by the Directive (see the reference made in art. 2 para. 1 of the Directive to Directives 95/46/EC, 2002/21/EC and 2002/58/EC) that have also been legally defined in national legislation?

No, not all of them. Below are the terms defined in Article 2(2) and their counterparts in the TD:

- **"Data"** (Article 2(2)(a) of the Directive): according to the Directive's definition, "Data" refers both to "traffic data" and "location data". The TD contains instead two separate definitions for "traffic data" (Article 1(1)(b)) and "location data" (Article 1(1)(c))

- "**User**" (Article 2(2)(b) of the Directive): the definition in Article 1(1)(a) TD matches that of the Directive, except for the parenthetical "for private or

business purposes", which does not appear in the TD. Please note that the definition of "User" in Article 4(2)(g) PDPC, instead, reflects entirely that of the Directive.

- **"Telephone service"** (Article 2(2)(c) of the Directive): Article 1(1)(d) refers instead to "phone traffic". The definition is equivalent to that in the directive but the reference to "calls (including voice, voicemail and conference and data calls)" is qualified by the parenthetical "as long as they are provided by a telephone provider"

- **"User ID"** (Article 2(2)(d) of the Directive): the definition in Article 1(1)(f) TD matches fully that in the Directive

- "**Cell ID**" (Article 2(2)(e) of the Directive): is defined neither in the TD nor in the PDPC.

- **"Unsuccessful call attempt"** (Article 2(2)(f) of the Directive): Article 1(1)(e) TD refers instead to "unanswered call". The definition is substantially equivalent to that in the Directive, but the language employed is slightly different.

Concerning the extent to what the definitions given therein differ from those in Article 2 par. 2, please, see the reply to the question above.

There are other terms mentioned in the Directive or in the directives referred to by the Directive (see the reference made in Article 2 par. 1 of the Directive to Directives 95/46/EC, 2002/21/EC and 2002/58/EC) that have also been legally defined in national legislation. National legislation also contains other terms defined in the directives referred to by Directive 2006/24/CE, as shown in the following table:

Term	Relevant EU provision	Relevant Italian provision
"personal data"	Article 2, par. 1, a) directive 95/46/CE	Article 4, par. 1, b) PDPC
"processing"	Article 2, par. 1, b) directive 95/46/CE	Article 4, par. 1, a) PDPC
"data processor"	Article 2, par. 1, e) directive 95/46/CE	Article 4, par. 1, g) PDPC
"persons in charge of the processing",	Article 2, par. 1, e) directive 95/46/CE	Article 4, par. 1, h) PDPC
"**data subject**"	Article 2, par. 1, a) directive 95/46/CE	Article 4, par. 1, i) PDPC
"**call"**	Article 2, par. 2, e), directive 2002/58/CE	Article 4**,** par. 2, b) PDPC
"**value added service**"	Article 2, par. 2, g), directive 2002/58/CE	Article 4, par. 2, l) PDPC
"**electronic mail**"	Article 2, par. 2, h), directive 2002/58/CE	Article 4, par. 2, m) PDPC
"**electronic communication network**"	Article 2, par. 1, a), directive 2002/21/CE	Article 4, par. 2, c) PDPC
"**electronic communication service**"	Article 2, par. 1, c), directive 2002/21/CE	Article 4, par. 2, e) PDPC
"**public communications network**"	Article 2, par. 1, d), directive 2002/21/CE	Article 4, par. 2, d) PDPC

Dimension 1 (State - citizen)

9. What data have to be retained according to the national rules transposing the Directive? Do these rules include additional retention obligations with regard to traffic data that go beyond the obligations mentioned in the Directive (e.g. location data resulting from the use of mobile email services), or do national retention obligations fall short of those specified by the Directive? Do data on unsuccessful call attempts have to be retained?

The types data to be retained for the purposes of Article 132 PDPC are set out in Article 3 TD:

1) Data necessary to trace and identify the source of a communication:

a) Concerning fixed network telephony and mobile telephony

- the calling telephone number
- the name and address of the subscriber or registered user

b) Concerning Internet access:

- name and address of the subscriber or registered user to whom an IP address, user ID or telephone number was allocated at the time of the communication

c) Concerning Internet e-mail:

- IP address and e-mail address and any additional user ID of the sender
- IP address and qualified domain name of mail exchanger host, in case of SMTP technology or other host relating to different technology

d) Concerning Internet telephony, fax, sms:

- IP address, telephone number and any additional user ID of the caller
- personal data of calling registered user

2) Data necessary to identify the destination of a communication:

a) Concerning fixed network telephony and mobile telephony

- the number(s) dialled (the telephone number(s) called) and, in case involving supplementary services such as call forwarding or call transfer, the number or numbers to which the call is routed
- the name(s) and address(es) of the subscriber(s) or registered user(s)

b) Concerning Internet e-mail

- e-mail address and any other user ID of the recipient
- IP address and qualified domain name of mail exchanger host, in case of SMTP technology or other host (relating to different technology), that has delivered the message
- IP address used for reception or consultation of e-mail by recipient

c) Concerning Internet telephony, fax, sms

- IP address, the telephone number and any other user ID of the recipient
- personal data of the recipient registered user
- further number(s) in case of supplementary services, as transfer of call

2) Data necessary to identify the date, time and duration of a communication:

a) Concerning fixed network telephony and mobile telephony, date and time of start and end of communication

b) Concerning Internet access

- date and time of log-in and log-off
- IP address (dynamic or static) assigned to communication by operator
- data for the identification of the subscriber or registered user

c) Concerning Internet e-mail

- date and time of connection and disconnection of user
- IP address

d) Concerning Internet telephony, fax, sms, mms

- date and time of connection and disconnection of user
- IP address

3) data necessary to identify the type of communication:

a) Concerning fixed network telephony

- the calling and called telephone numbers

b) Concerning mobile telephony

- the calling and called telephone numbers
- the International Mobile Subscriber Identity (IMSI) of the calling party
- the International Mobile Equipment Identity (IMEI) of the calling party
- the IMSI of the called party
- the IMEI of called party in the case of pre-paid anonymous services, the date and time of the initial activation of the service and the location label (Cell ID) from which the service activated

c) Concerning Internet telephony, fax, sms, mms

- the calling telephone number for dial-up access
- the digital subscriber line (DSL) or other end point of the originator of the communication

4) Data necessary to identify the location of mobile communication equipment

- the location label (Cell ID) at the Article of the communication
- data identifying the geographic location of cells by reference to their
- location labels (Cell ID) during the period for which communications data are retained

The data retention obligations laid down in the TD are significantly more detailed than those set out in the Directive. For instance, while some provisions of the Directive require the retention of the same categories of data for different types of communications, the TD breaks down that requirement, and details different categories of data to be retained for each type of communication. Moreover, in addition to the Directive requirements, various provisions of the TD also mandate the retention of "any additional user ID".

Data on unsuccessful call attempts must be retained for a period of 30 days (*see* Article 132, par. 1-bis PDPC). That obligation was subject to a three month transitional period (*see* reply to question no. 6)

10. Does national law otherwise provide for, or allow for, the retention of electronic communications data (customer records, traffic data and/or the content of communications) beyond the data to be retained in accordance with the Directive? Please specify the substance of these provisions.

The PDPC allows providers to *process* the traffic data necessary for billing purposes (also in the case of interconnection fees) for a period not exceeding 6 months. That data can be relied upon as evidence in case the bill is challenged or payment is to be

pursued. That provision is without prejudice to the additional retention necessary on account of a claim lodged with judicial authorities (Article 123, Par. 2 PDPC).

11. According to the national rules transposing the Directive, for which purposes is data retention mandated in each case?

As a rule, according to the TD and the PDPC data retention is allowed only for the purpose of 'detecting and suppressing criminal offences'. That wording refers to the process of establishing that a crime has been committed and punishing the wrongdoer for that crime, it does not involve any *preemptive* or ex ante action.

Traffic data, moreover, can also be processed for billing and for interconnection payments (see reply to question no 10)

12. Are there any specific rules in national law prohibiting the retention and/or transmission of sensitive data (i.e. data that is legally considered to be particularly worthy of protection, e.g. data resulting from a communication between individuals that are in a relationship of mutual trust particularly protected by law for reasons of overriding importance, as might be the case between a lawyer and his/her client, between a doctor and his/her patient, between a journalist and a whistle-blower)?

There is no general framework governing the *retention or transmission* of sensitive data, but a number of sector-specific sets of rules governing various facets of the matter. First, it is worth reminding that the PDPC sets out the relevant provisions concerning the *processing* of sensitive data, as well as specific requirements for public authorities and private parties. The former can process sensitive data only if so expressly empowered by a legislative provision specifying the types of data that can be processed and the general interest goal to be pursued (see Articles 18-22 PDPC). Private subjects, instead, can only process sensitive data with the consent of the persons concerned and following authorization by the Garante (see Articles 23-27 PDPC). General rules as to the processing of sensitive data are set out in Article 22 PDPC.

Moreover, it must be noted that sensitive data are often subject to the provisions on secrecy set out in Articles 200-204 and Article 256 of the Code of Criminal Procedure ("CCP").

(see http://www.camera.it/_bicamerali/leg15/sis/norme/cpp.htm).

Article 200 CCP deals with professional confidentiality. It provides for that, as a rule, religious ministers, lawyers and experts, medical doctors pharmacists and nurses, and other professionals cannot be required to testify about facts they learnt by reason of their office, ministry or profession. Likewise, professional journalists cannot be required to divulge the identity of their informers, unless that is strictly necessary to the solution of the case pending before a court.

Article 201 CCP deals with the legal privilege vested in public officers, servants and the like. Article 202 CCP provides for that the subjects referred to in Article 201

CCP can refuse to testify on matters covered by the secret of State.

In any case, in accordance with the principle of secrecy of correspondence laid down in Article 15 of the Italian Constitution, the PDPC excludes the retention of *the contents of communications* (Article 132 PDPC).

13. **For how long do the data retained in accordance with the national rules transposing the Directive have to be kept available? In case a distinction is made according to data categories: Please describe the criteria the distinction is based upon and the reasons therefore.**

According to Article 132, par. 1 PDPC, **telephone traffic** data must be retained by the provider for 24 months as from the date of the communication with a view to detecting and suppressing criminal offences For the same purposes, **internet traffic data**, not including the content of communications, must be retained by the provider for 12 months as from the date of the communication.

As per Article 132, par. 4-ter PDPC, the Minister of Home affairs and a number of law enforcement agencies, also in connection with requests lodged by foreign investigating authorities, may, for the purposes of crime prevention or pre-trial investigations, require ISPs to retain and protect Internet activity data, except for the contents of data, for a period no longer than 90 days. That term may be extended up to 6 months.

Pursuant to Article 132, par. 1-bis, the data related to **unsuccessful calls** that are temporarily processed by the providers of publicly available electronic communications services or a public communications network must be retained for 30 days.

It is thus apparent that, as a general rule, electronic communications traffic data are retained for a lower period relative to telephone traffic. This because electronic communications data traffic are more sensitive, in that they can disclose, indirectly, the content of communication or relevant information, increasing the risks of profiling (cf. Recital 1 TAD*)*

14. **Which authorities or other bodies are entitled to access the data retained (e.g. law enforcement agencies, security authorities and/or intelligence, other public bodies, (private) claimants/litigants)?**

The subjects entitled to access retained data are law enforcement and prosecutorial agencies, the counsels for either the defendant or the person under investigation (see Article 132(3) PDPC). Foreign investigating authorities may request Italian authorities (the Ministry of Internal affairs etc.) to order service providers to retain data for investigation purposes (Article 132(4 ter) PDPC)

15. **For which purposes may the data retained be used according to the national law transposing the Directive, for which purposes may they be used according to other national law (e.g. for law enforcement (criminal/administrative offences), security, civil action (e.g. to enforce copyright claims))? Does the**

national law grant any rights to individuals to access the data retained directly, e.g. in a civil action (right to information on the owner of an IP address)?

According to the PDPC as amended by the TD, retained data can be used in order to detect and suppress criminal offences, as well as for the purposes of pre-trial investigations, the prevention of terrorist crimes etc.

Individual access, for instance in the framework of copyright enforcement, is also allowed. However, a distinction must be drawn between criminal and civil proceedings. In the case of criminal proceedings, courts, following a substantiated claim by the party concerned, can order the communication of all data relating to the violation, including personal data. In the case of civil actions, instead, traffic data cannot be disclosed to individual parties.

The *Garante* has expressly stated that courts are under no obligation to disclose traffic data in the context of civil, administrative and accounting disputes (see Garante Decision of 19 September 2007 and Recital 5(a) TAD). In its Decision of 28 February 2008, moreover, the *Garante* outlawed the use by private companies of a software designed to monitor, for the purpose of identifying and suing them, the activities of peer-to-peer (P2P) users that share copyrighted files on the Internet.

Turning to Italian courts, the Constitutional Court in 2006 held that the right to privacy, as a fundamental right, must take precedence over other personal interests of lesser constitutional relevance, but must yield to the need to protect the community from serious criminal offences (Const. Court, judgment no. 372/2006). The application of that principle by lower courts, however, has not always been consistent. In a well known line of cases (the "Peppermint case"), some record companies brought proceedings before the Rome Civil Court of First Instance seeking an order that the relevant ISPs be enjoined to disclose the identities of the users behind the IP addresses logged by the applicants through a proprietary software. The earliest cases were decided in favour of the record companies, which promptly contacted the users concerned requesting that they pay a sum to settle the claim or face the consequences of criminal proceedings. In subsequent judgments, however, following the intervention in the proceedings of the consumer association Adiconsum and of the *Garante* itself, the Rome Court reversed its earlier case-law and dismissed the applicants' claims. (*see* A. Arena, Monitoring the Activities of P2P Users Runs Foul of Privacy Legislation*, in* Iris - Legal Observations Of The European Audiovisual Observatory, n. 7/2008, p. 26; cf. Court of Rome, judgment of July 16, 2007).

16. **Which specific requirements have to be fulfilled in order to access the data for one of the purposes mentioned in question 15 (e.g. a suspected serious crime, specific risks to public safety)?**

Italian law does not provide specific requirements in order to access the data concerned other than those mentioned in the reply to question 15.

17. Is it required to obtain a court order before accessing the data retained? Is it required to hear the aggrieved party or to involve him/her otherwise in the proceedings before data is accessed?

Data can be acquired from the provider by means of a reasoned order issued by the public prosecutor as well as upon request by the counsel for the person under investigation, the defendant, or the injured party. The counsel for defendant or the person under investigation is empowered to directly request traffic data from the provider with regard to the data related to "the subscriptions entered into by his/her client" (Article 132, par. 3 PDPC).

Moreover, the PDPC does not set out an obligation to hear or to involve the aggrieved party before data are accessed.

18. Is it provided for by law that the aggrieved party shall be notified of a data access? As a rule, does this notification have to be effected prior to or after the data access? Under which conditions is it allowed to deviate from this rule?

The PDPC does not set out an obligation to notify the aggrieved party before data are accessed.

19. Does the aggrieved party have a right to be informed about the data accessed as far as they are related to him/her?

The PDPC does not set out a specific information obligation, but as per Article 7 thereof individuals have the right to obtain confirmation as to whether or not personal data concerning them exist. Nonetheless, that right cannot be exercised if data are processed by courts for judicial reasons (Article 8, par. 2, e) PDPC), as in that case even the prior consent requirement is waived (Article 24, par. 1, f) PDPC).

20. May the aggrieved party have recourse to the courts for the (intended and/or already effected) data access? Which remedies do the aggrieved party dispose of? What rights does the aggrieved party have in the case of an unlawful data access or processing operation?

The law does not provide for specific arrangements in this respect, but the aggrieved party can bring proceedings to obtain compensation for damages deriving from unlawful data processing on the basis of Article 2050 of the Civil Code (exercise of dangerous activities) (see Article 15 PDPC).

21. Are there any legal provisions protecting the data retained against unauthorised access in a particular way (not: purely technical guidelines or organisational measures, see question 40 d) in this regard)? Please describe the content of these provisions.

The particular character of retained data calls for specific forms of protection. Article 132, par. 5, PDPC stipulates that the processing of that data be carried out in accordance with the principles set out in Article 17 PDPC, i.e. in compliance with specific "measures and arrangements" laid down by the *Garante* in accordance with

the general principles underpinning the PDPC. Moreover, data processing must be carried out in accordance with the security requirements set out in Articles 31-36 PDPC as well as with the technical guidelines in Attachment B to the PDPC (page 181 of the English version).

Technical requirements and organizational measures are instead addressed in the replies to question no. 40 (a) – (g).

22. When do the accessing bodies have to destroy the data transmitted to them?

While rules are in place to require providers *retaining* the data to destroy them once the compulsory retention period is over, there are no rules on this matter for bodies *accessing* the data. Nonetheless, Article 11, par. 1, lit. e) PDPC provides for that personal data that permit the identification of the subject must not be kept for longer than is necessary for the purposes for which that data were accessed or subsequently processed.

Dimension 2 (State – economy)

23. Which private bodies/enterprises (e.g. internet service providers) are obligated to retain the data? Please distinguish the group of obligated parties from providers of neighbouring services.

Article 132 PDPC sets out a number of retention requirements for "providers" (par. 1, concerning telephone traffic data and electronic communications traffic data), "providers of publicly available electronic communications services or a public communications network" (par. 1-bis), and "IT and Internet service providers" (par. 4-ter and 4-quarter).

Regrettably, the notion of "provider" is defined neither in the PDPC nor in the TD. It must be noted, however, that Article 132 is placed in Title X, Chapter I of the PDPC, entitled "Electronic communication services". The first article of that Chapter, Article 121 (entitled "Services concerned"), provides for that "this Title shall apply to the processing of personal data in connection with the provision of publicly accessible electronic communication services on *public* communications networks" (emphasis added). It follows that the addressees of the requirements set out in Chapter I, including Article 132 above, do not include subjects involved in the operation of *private* communication networks.

Additional guidance as to the notion of "provider" can be gleaned from Recital no. 3 of the TAD, which reads as follows:

The "providers" required to retain traffic data under section 132 of the Code are those making electronic communications services available to the public on public communication networks. "Electronic communication services" are services consisting, whether wholly or mainly, "in the conveyance of signals on electronic communications networks" (Section 4(2) letters [d) and e) of the PDPC]).

[...] Hence, the requirement to retain data applies, under section 132 above, to the entities that bring into effect, whether exclusively or not, the conveyance of signals on electronic

communications networks – irrespective of the proprietary status of such networks – and offer services to end-users in pursuance of the non-discrimination principle (see also directive 2002/21/EC and decree no. 259/2003 – Electronic Communications Code.)

24. Within the group of parties obligated in principle to retain data, are there some who are (by law) or may be (upon request) exempt from these obligations, e.g. non-commercial service providers or service providers with a minor turnover/market share?

Recital no. 3 TAD is the main authority as to the categories of subjects that are exempt from data retention requirements:

- **Entities directly offering electronic communication services to *limited groups of individuals*** (e.g. public or private bodies that only enable their employees and/or collaborators to carry out telephone or Internet communications). Although these services fall within the scope of the general definition applying to "electronic communication services", they cannot be regarded as services "available to the public" and are thus exempt from the retention requirements. Nonetheless, if the communication is routed to a user outside a "private network", the traffic data generated by that communication must be retained (for instance, this applies to the provider used by the recipient of the communication in question, in case the latter consists in an e-mail message: see, on this point, document WP37 "Protection of Privacy on the Internet" of 21 November 2000, available at: http://www.garanteprivacy.it/garante/document?ID=434621);

- Entities that *do not directly generate or process traffic data* even though they offer publicly available electronic communication services;

- **Owners and managers of public establishments and/or private clubs of any kind that only make terminals available to the public, or to customers and/or associates**, whereby such terminals may be used for telephone or Internet communications, or else that make Internet wireless access points available to the public (except for public payphones that only operate in voice mode). It is worth noticing, however, that those guidelines must be read in connection with the obligations set out by Ministerial Decree August 16, 2005 (http://it.wikisource.org/wiki/D.M._16_agosto_2005) implementing Article 7, par. 4 of Law no. 155/2005 (Urgent measures against international terrorism, available at http://www.camera.it/parlam/leggi/05155l.htm). According to the Ministerial Decree, managers of private circles or public establishments which make terminals enabling connection to the internet by the general public, members or customers, are required *inter alia* to identify the users of those terminals and to retain data as to the hours of use of those terminals, excluding the contents of the relevant communications.

- **Managers of Internet websites disseminating contents on the Web (so-called "content providers")**. They do not provide an "electronic communication service" as per Article 4, par. 2, letter e) of the PDPC – which in turn refers to Article 2, par. c) of Directive 2002/21/EC, whereby "the services providing

contents conveyed by means of electronic communication networks and services" are excluded from the scope of the Directive. Additionally, it should be pointed out that traffic data related to a communication – such as navigation data and the pages visited on website – often allow detecting or disclosing the contents of such communication; accordingly, retaining such data would be actually in breach of section 132 of the PDPC, which does not require the "contents" of communications to be retained, even for judicial purposes (see also article 1(2) of directive 2006/24/EC, whereby retention of the "content of electronic communications, including information consulted by an electronic communications network" falls outside the scope of the directive);

- **Search engines**. The Internet traffic data processed by search engines allow tracking of the operations performed by users on the Web and can be equated to "content" data, which must not be retained (see above).

25. Which of the data categories that have to be retained according to the Directive have already been retained by the obligated parties before the Directive entered into force, e.g. for billing or other business purposes or in order to comply with (other) legal obligations?

At the outset, it must be noted that prior to the entry into force of the TD, the Italian law on the subject of data retention resulted from an intricate patchwork of partly overlapping provisions, a succession of transitory periods, and a number of unimplemented commitments. Turning to the subject addressed in the question, the first provisions on that matter were set out in Legislative decree no. 171/1998 (concerning the contract relationships between providers and users). Article 4, par. 2 thereof provided for that providers could retain *telephone calls data for billing purposes* until such time as the bill or the outstanding fees become unenforceable. Subsequently, Legislative Decree no. 196/2003 required the retention of *traffic data for billing purposes* (Article 123 PDPC) *as well as for the detection and suppression of crimes*. That retention requirement was then extended to *Internet traffic data* as per Decree-Law no. 144/2005, converted into Law no. 155/2005.

26. Are there any legal obligations on data security in place other than those mentioned in your answer to question 21 (e.g. rules on data quality, on system stability and reliability, against unauthorised destruction, loss or alteration of the data)?

Apart from the arrangements referred to in the replies to question no. 40 (a) – (g) and to question no. 21 there are no other legal obligations on data security.

27. Which *additional* costs (i.e. costs over and above those arising from the retention of the data categories specified in your answer to question 25) originate in total from the implementation of the national law transposing the Directive (i.e. aggregate figures of all obligated parties in your country as a whole)?

Unfortunately, no estimate of the overall costs arising from the implementation of the data retention rules has been released yet.

28. Do the obligated parties receive reimbursement for their costs by government? If so: Which costs are reimbursed (only costs for disclosure of retained data or also costs for investment into the required storage technology and/or costs to ensure data security and separate data storage)? What legal requirements have to be met for an obligated party to be eligible for cost reimbursement?

The TD contains no reference to an addressee's right to reimbursement for the costs incurred in complying with the new framework. The unavailability of a reimbursement claim is confirmed in Article 6 TD, expressly stating that the implementation of the rules set out in the TD must not result in new or greater burdens for the public purse. Public entities and agencies must comply with the TD rules with their existing human, financial, and technical resources.

29. What (statutory) rules are in place governing co-operation between the party retaining the data and the party (public authority) accessing them?

Apart for the procedural requirements set out in Article 132, par. 3 PDPC (see the reply to question no. 17), the co-operation between the party retaining the data and the public authority accessing them, to date, is not the subject of statutory rules, but rather of informal arrangements on a case by case basis.

30. Does the national law provide for any sanctions (e.g. administrative or criminal penalties) and/or obligations to pay compensation for damages suffered in case of an infringement of data retention provisions by the obligated parties? Please describe the content of these rules.

As per Article 162-bis PDPC, any violation of the PDPC provisions as amended by the TD are punishable by an administrative fine ranging from Euro 10,000 to 50,000, unless the facts at issue constitute a criminal offence.

Article 5, par. 2, TD further provides for that the allocation of an IP address unable to univocally identify the user is punishable by an administrative fine ranging from Euro 5,000 to 50,000, which can be tripled in relation to the economic conditions of the subject. The Ministry for Economic Development is responsible for the establishment of infringements and the application of those sanctions (subject to judicial review by courts).

Moreover, as mentioned in the reply to question 20, damages suffered as a consequence of the violation of data retention provision can give rise to a civil action as per Article 2050 of the Civil Code.

Dimension 3 (State – State)

31. Which public body is responsible for establishing the contact with the party retaining the data in order to actually access that data when an entitled body (see question 14) so wishes?

Apart for the procedural requirements set out in Article 132, par. 3 PDPC (see the replies to question nos. 14 and 17), the PDPC does not further regulate this matter.

32. Are there any regional entities (e.g. constituent states/federal states, autonomous regions or the like) vested with own authority that have been granted their own rights of access (in addition to those of the central state/federal state) to the retained data?

As per Article 117(1)(h) of the Italian Constitution, the Central Government has an exclusive competence over law enforcement matters, except for local administrative police, whose tasks, however, have little to do with criminal matters. Regions, therefore, do not have their own prosecutors. Accordingly, there is no provision of a right of access to retained data by regional authorities.

33. What (legal) rules are in place governing co-operation among the different bodies accessing the data and between these and other public authorities (in general as well as in particular as regards the exchange of the retained data)? Have general rules of co-operation been adapted in the course of the Directive's transposition?

There are no specific rules on this matter. General rules governing co-operation between administrative authorities include the principle of 'good administration' (buona amministrazione) as per Article 97 of the Italian Constitution. Law no. 241/1990 also sets out general principles governing administrative procedures, including efficiency, transparency etc. and procedures involving more than one administration (Articles 14 ff.)

34. On what legal basis does the exchange of retained data with other EU Member States, other EEA Member States and (if permitted) third countries (e.g. CoE Member States party to the Cybercrime Convention) take place? Do foreign state bodies avail of a right (vis-à-vis the obligated party) to access the retained data directly? If the answer is negative: Which (national) authorities are responsible for cross-border data exchange (the conveyance of outgoing requests and the processing of (responses to) incoming requests)?

The PDPC does not lay down a specific framework for the exchange of retained data with other EU Member States, except for the rules set out in Article 42 PDPC, whereby no provision of the PDPC must be applied so as to restrict or prohibit the free movement of personal data among EU Member States. Nonetheless, PDPC rules can be applied if data are transferred to other EU Member States with a view to escaping the PDPC rules. Due to the vagueness of the wording of that anti-circumvention provision, doubts arise as to its compatibility with the right of establishment and the freedom to provide services as per the Treaty on the Functioning of the European Union.

Turning to the transfer of data to Third countries (i.e. outside the EU), Article 45 PDPC provides for that, as a general rule, such transfer is prohibited, even if it occurs on a temporary basis and irrespective of its forms and means, if the laws of the country of destination or transit of the data do not ensure an adequate level of protection of individuals. In this connection, account must be taken of the methods used for the transfer and the envisaged processing operations, the relevant purposes, the nature of the data and the security measures employed. Article 43 PDPC lays

down a number of requirements for the transfer of data to Third countries, such as the necessity of obtaining the consent of the person concerned, which must be expressed in writing if the data at issue are of a sensitive nature.

Moreover, Article 132, par. 4-ter PDPC provides for that, in order to address the requests submitted by foreign investigation authorities, the Minister for Home Affairs or the heads of the central offices specialising in computer and/or IT matters from the State Police, the Carabinieri, and the Financial Police may order IT and/or Internet service providers and operators to retain and protect for no more than 90 days Internet traffic data, except for contents data, in order to carry out pre-trial investigations or else with a view to the detection and suppression of specific offences.

35. Which are the bodies in charge of monitoring compliance with the national rules (including, but not limited to, those on data security pursuant to Articles 7 and 9 of the Directive) by all parties involved? Do these authorities act with complete independence or do they exercise their functions under the supervision of a superior authority or ministry? Which kind of supervision is applied (comprehensive supervisory control in terms of both legality and technical advisability or supervision limited to the control of legality)?

Article 154, par. 1, lit. a) PDPC expressly empowers the *Garante* with the task of monitoring compliance with the applicable rules on the subject of data processing and data retention activities. Those rules include the relevant national provisions, as well as unconditional and sufficiently precise provisions laid down in EU directives and other directly applicable EU rules (see Judgment of the Court of Justice of 22 June 1989, *Fratelli Costanzo SpA v Comune di Milano*, Case 103/88, ECR 1989 p. 1839). That duty is expressly codified in Article 154, par. 2, PDPC, albeit no reference is made to Directive 2006/24/EC.

The Garante is an independent authority (see Article 153, par. 1). As such, it is accountable only to the Parliament, whose two Houses are responsible for the appointment of the Garante's four board members. In this connection, it must be noted that as per Article 154, par. 1, lit. m) the Garante must report once a year to the Government and to the Parliament on its activities and on the implementation status of the PDPC.

Moreover, each year, the parties retaining data are required to report to the Ministry of Justice, which in turn will forward these information to the European Commission, on the total number of cases in which telephone or internet traffic data have been transmitted to the relevant authorities, the interval between the storage of the relevant data and the request by the relevant authorities, and the cases where access applications have been rejected (Article 4, par. 2 TD).

II. Relevant case-law

36. Are there any lawsuits or administrative proceedings – pending or concluded by a final adjudication – concerning the legality of the national law transposing the Directive or parties thereof?

To the author's best knowledge there are no pending judicial or administrative proceedings concerning the legality of the national transposition provisions.

For the sake of completeness, it must be noted that the constitutionality of the wording of Article 132 PDPC in force prior to the amendments by the TD was reviewed by the Italian Constitutional Court in its judgment no. 372 of 14 November 2006. On that occasion, the Court held that the said PDPC provision had struck a "fair balance" between the individual right to privacy and the common interest to the suppression of serious crimes.

If so, please answer to the following questions:

a) Who are the plaintiffs/claimants and the defendants/respondents?

/

b) Which legal norms claimed to be in conflict with the challenged law do the plaintiffs/claimants base their motion upon?

/

c) Please describe briefly the outcome of concluded proceedings and the essential grounds of the rulings issued. Do these rulings seek to reach a balance of the interests protected by fundamental rights and, where applicable, other norms enshrined in the constitution or having constitutional status? Do the rulings make reference to previous case-law that deals the legitimacy of other collections of personal data?

/

37. Are there any lawsuits – pending or concluded by a final adjudication – with European courts (e.g. ECtHR, ECJ) concerning the legality of data retention obligations in which your Member State is/was involved (the indication of the case number is sufficient)?

There are currently no lawsuits pending before the ECJ or the ECtHR concerning the implementation of Directive 2006/24 in Italy.

III. State of play of the application of the national law enacted to transpose the Directive

38. Where are the data stored (e.g. at the service providers' premises, with external companies, with the State)? Are the data stored locally or at a centralised level?

Data are stored by each provider either locally or in a centralized fashion (Recital (7)(1) TAD).

39. Are data stored outside the country or would this be permissible according to national law? If either of these cases applies: what data protection rules have the companies involved in the storage (both in your country and abroad) been obligated to?

The PDPC provisions apply also to data stored abroad, as clarified in Article 5 PDPC which provides for that its provisions apply "to the processing of data, also stored abroad, by whoever is established in the territory of the [Italian] State or in a place subject to the sovereignty thereof"

Moreover, the PDPC lays down a number of provision on cross-border data flow (see Articles 42-45 PDPC). By and large, data transfer to EU countries is always allowed, safe in the case of circumvention; whereas, data transfer to non-EU countries is subject to a number of requirements and, at any rate, is not allowed if the laws and regulations of the host State does not ensure an adequate level of protection of individuals. See the reply to question no. 34 for further details.

40. Which technical and/or organisational measures ensure in practice that

a) no data are retained beyond what is permitted?

In order to ensure that data are not stored beyond what is permitted, Italian law provides for i) technical and organization measures (which will be addressed in greater detail in the answers to the questions below) and ii) internal audit arrangements.

In this connection, regard must be had, first and foremost, to the detailed requirements set out by the Garante in the TAD. Article (a)(6) thereof, in particular, mandates the implementation of solutions that can ensure **supervision over the processing of traffic data** by the individual persons in charge of the processing – irrespective of their positions, skills and tasks as well as of the purposes of the processing. The supervision in question must be effective and accurate as also related to the processing operations performed on the individual items of information held in the various databases. The solutions referred to above include storage, in an ad-hoc audit log, of the operations performed (whether directly or indirectly) on traffic data and any other personal data related thereto. This applies both to the operations consisting in and/or deriving from the interactive use of the systems and to the operations performed via the automatic functioning of IT software. Audit log systems must ensure that the records they

contain are complete, non-modifiable, and authentic with regard to all the processing operations and all IT-security-related events being audited. To that end, storage systems on non-modifiable devices must be implemented to record auditing data – possibly in a centralised fashion – from the individual processing facilities and/or data centres. The data and/or data clusters must undergo computerised procedures prior to being written in order to certify their integrity; encryption technology must be used in the said procedures.

Article (a)(7) of the TAD, further requires that **internal auditing** procedures be carried out at least at annual intervals in order to monitor compliance with organisational, technical and security measures as applying to traffic data in pursuance of the legislation in force as well as of the PDPC's provision, including the measures that are required to select the persons in charge of this specific processing. This type of audit should be committed to a corporate unit and/or staff that should be other than those in charge of processing the data for the purposes of detecting and suppressing crime. The auditing activity must include ex-post checks, sample checks and/or alarm-triggered checks based on alerting and anomaly detection systems; checks on lawfulness and legitimacy of data access by the persons in charge of the processing; checks on data integrity; and checks on the computerised procedures implemented for data processing. Regular audits should be also carried out on the actual erasure of the data upon expiry of the relevant retention periods. The auditing activity must be documented as appropriate in order to always enable establishing which systems have been audited, which technical operations have been performed, which findings have resulted from access analysis, and which criticalities have been detected. The outcome of the audits must be i) disclosed to the individuals and bodies that are empowered to make decisions and implement corporate policies (based on the respective organisational status); ii) referred to in the security policy document, which must specify the actions required, if any, to upgrade security measures; and iii) made available to the Garante and judicial authorities, if they so request.

b) where so required, the necessity to obtain a court order before accessing the data is duly observed and that State bodies otherwise cannot get access to the data (e.g. technical measures inherent to the system)? Are there any technical interfaces enabling State bodies to access the data directly (even if this may be illegal)?

The PDPC does not lay down technical arrangements to ensure that State bodies cannot obtain access to retained data in the absence of a Court order.

c) data are not used for purposes other than those they are permitted to be used?

This issue is addressed in Article (a)(3) of the TAD by requiring **segregated storage arrangements**. According to that provision, as to traffic data that are retained exclusively for the purpose of detecting and suppressing criminal offences, the TAD requires the implementation of IT systems that are physically

different from those used to manage traffic data for other purposes. This applies to both processing and storage components. Conversely, traffic data that are retained for no longer than six months after being generated may be processed for justice-related purposes both by means of the same processing and storage systems used for processing operations in general and by duplicating them and keeping them separate from the traffic data that are processed for standard purposes. Moreover, the IT equipment that is used to process traffic data exclusively for justice-related purposes must be placed inside restricted access areas and there must be electronic control devices and/or supervisory procedures in place in those areas so as to allow recording of the identification data related to access-enabled individuals including the respective time frames. If telephone traffic data are processed exclusively for justice-related purposes, access control must envisage biometric recognition procedures. Finally, there must be suitable measures in place to restore access to the data if the latter and/or the electronic tools are damaged; the time required for this purpose must be compatible with data subjects' rights and should in no case be in excess of seven days.

d) data are protected against unauthorised or unlawful (deliberate or accidental) storage, processing, access or disclosure, destruction, loss or alteration (cf. questions 21 and 26; e.g. through encryption, physical protection, application of the four-eyes principle along with secure authentication, local/decentralised storage etc)? Please describe the measures taken both by the party retaining the data and by the party accessing them.

In order to ensure protection against unlawful against unauthorised or unlawful (deliberate or accidental) storage, processing, access or disclosure, destruction, loss or alteration, apart from the minimum security measures concerning authentication set out in Annex B to the PDPC (page 181 of the English edition) the TD sets out a number of different arrangements. These include:

- computerised authentication systems that must be based on **strong authentication techniques** (Article (a)(1) TAD);

- specific procedures to ensure **separation between the allocation of authentication credentials** and identification of authorisation profiles, on the one hand, **and technical management of systems and databases**, on th other hand (Article (a)(2) TAD);

- the **appointment of persons** in charge of data processing that have attended regular training sessions (Article (a)(4) TAD);

- **IT solutions that can ensure supervision over the processing** of traffic data by the individual persons and cognizability of each and every processing operation performed on the individual items of information held in the various databases (Article (a)(6) TAD);

- **Encryption** of data processed for justice-related purposes (Article (a)(9) TAD);

Encryption protocols deserve a closer scrutiny at this juncture, insofar as Article (a)(9) TAD expressly acknowledges the risk that justice-related data may be acquired and/or altered accidentally in the context of maintenance operations or in the course of standard system administration operations. Hence, the TAD requires that providers make arrangements to prevent the information contained in the databases that are used by the IT applications deployed for the processing in question from being intelligible to any entity that does not fulfil the appropriate access conditions and/or authorisation profiles. To that end, encryption and/or obfuscation of database parts and/or indexes and/or other encryption-based technical measures can be implemented. The above arrangements must be effective in order to minimize the risk that persons in charge of technical activities related to the processing – e.g. system administrators, database administrators, hardware/software maintenance engineers – might get undue access to the stored information – perhaps by chance – in the course of accessing the systems in question and/or performing maintenance activities, or that they might modify the stored information whether intentionally or not. Traffic data flows between the provider's information systems must take place via secure, encryption-based communication protocols; in any case, no plaintext data should be transmitted. Secure communication protocols must also be implemented to ensure, generally speaking, system security – in particular, to prevent vulnerability and intrusion risks.

e) data are destroyed safely (i.e. irrevocably) and immediately upon expiry of the retention period provided for by law?

Upon expiry of the terms set out in the legislation in force, traffic data must be made unavailable to processing and retrieval by IT systems; they must also be deleted or made anonymous without delay, within a time limit that must be technically compatible with implementation of the relevant IT procedures – this applies both to the databases and processing systems used for processing and to the backup and disaster recovery systems and media, also pursuant to the measures set out in the legislation in force. The operations in question must be documented by no later than thirty days as from expiry of the terms mentioned in Article 132 of the PDPC (Recital 7(5) and Article (a)(5) TAD).

f) the aggrieved parties are notified accordingly, if this is provided for by national law (e.g. technical measures inherent to the system, specific assignment of the task to staff, cf. question 18)?

As mentioned above, Italian law does not provide for a duty to notify the aggrieved parties about data access.

g) sensitive data (cf. question 12) are not retained or transmitted, respectively, as far as this is provided for by national law?

This issue is dealt with in paras 20-24 of Annex B to the PDPC (page 181 of the English version).

Sensitive or judicial data must be protected against unauthorised access as per

Article 615-ter of the Criminal Code (whereby unauthorized access to secure networks is punishable up to 3 years of imprisonment) by implementing suitable electronic means. To this end, organisational and technical instructions shall be issued with regard to **keeping and using the removable media** on which the data are stored in order to prevent unauthorised access and processing. The removable media containing sensitive or judicial data shall be destroyed or made unusable if they are not used; alternatively, they may be re-used by other persons in charge of the processing, who are not authorised to process the same data, if the information previously contained in them is not intelligible and cannot be re-constructed by any technical means. If either the data or electronic means have been damaged, suitable measures shall be adopted to ensure that data access is restored within a specific deadline, which must be compatible with data subjects' rights and not in excess of seven days. In the Security Policy Document (*Documento programmatico sulla sicurezza*) are be contained the specification of the criteria to be implemented in order to either encrypt such data or keep them separate from other personal data concerning the same data subject.

41. Is there an effective control that the measures referred to in question 40 are effectively applied (e.g. data protection audit, (in-house or public) data protection officer, external auditors)?

Compliance with the measures referred in question 40 is ensured by a twofold audit system, encompassing both internal audits (see the reply to question 40, lit. a) and external monitoring carried out by the Garante as per Article 154, par. 1, lit. c) PDPC.

In order to facilitate the Garante in its external supervision task, Article (a)(8) TAD requires providers to **document the information systems** used to process traffic data as appropriate in accordance with software engineering principles. Non-standard and/or non-commonly received descriptions should be avoided. For each application system, the description should refer to the logical/functional architecture, the overall architecture and structure of processing systems, traffic data input/output flows, the communication network architecture, and the entities/categories authorised to access the system. The documentation in question should come with location diagrams of applications and systems to show the specific location of the individual systems where the data used for detecting and suppressing criminal offences are processed. The technical documentation must be updated and made available to the Garante, upon request, along with detailed information on the entities authorised to access the systems with a view to processing traffic data.

42. What technical (*de facto* and/or *de iure*) standards are applied with respect to data retention and transmission? Have the operational systems used been designed in such a way that interoperability is ensured? How is it ensured that security standards are adjusted to the current technological state of the Article?

Technical standards must keep up with state-of-the-art technology, hence they are routinely updated by the Garante (Recital 7 TAD). Compliance with those standards is first and foremost ensured by the internal audits each provider is required to carry out as per (Article (a)(7) TAD). Moreover, the Garante carries out external monitoring as per Article 154, par. 1, lit. c) PDPC and can benefit from the documentation obligations each provider is subject to as to the state of its systems as per Article (a)(8) TAD.

43. How is co-operation between the party retaining the data and the party accessing them effected in practice? Please describe the procedure of data transmission from the retaining to the accessing party.

No formal guidelines or codes of conduct have been yet adopted on the subject to the co-operation between the party retaining the data and the party accessing them. Access requests are handled on a case-by-case basis. Usually, the criminal prosecutor (Pubblico Ministero) in charge of the investigation issues a reasoned decision (decreto motivato) requesting the party retaining the data to disclose information relevant to a criminal investigation. The retaining party, in general, takes one week to four months to comply with that decision.

44. According to which procedure are cross-border requests issued or responded to, respectively? Is/are there (a) common working language(s) used in this context?

There are no formal standards or protocols on this specific matter.

B. National (societal) context

45. In general, is society aware of the public surveillance measures adopted in your country? How are these measures assessed by citizens, economy, the government and other public bodies? Please describe the public debate on the introduction (and, if corresponding rules have existed before the Directive entered into force, also on the amendment) of data retention in your country. Please illustrate the situation as comprehensively as possible, i.e. differentiating by political and social groups (political parties, civil rights groups, labour unions as well as other professional organisations of the professions concerned (police officers, judges, lawyers/attorneys), consumer and business associations, the media, etc), and by the parties involved (businesses, data protection officers, law enforcement agencies, government representatives).

The implementation of the Directive has given rise to considerable controversy

among stakeholders, legal expert, and academics.
Providers, in particular, have insisted on the substantial compliance costs they have to bear in order to comply with the transposition measures. The Garante, which launched broad consultations on the issue of data retention more than a year before the Directive's transposition into Italian law (see http://www.garanteprivacy.it/garante/doc.jsp?ID=1442530), was receptive to those claims, and in the case of small and medium-sized undertakings it took steps to ensure that requirement compliance can be carried out at cost-oriented prices (see hyperlinked article).
Consumers associations, in turn, have reported that user personal data are routinely processed disregarding the applicable laws and regulation, with a serious risk for the privacy of users. Italian consumers associations, accordingly, have joined fellow organizations from other Member States in a petition to the European Commission to abolish the retention requirement for traffic data (see hyperlinked article).

46. Are there any obligations in your country to retain other personal data without a specific reason (e.g. passenger name records (PNRs), employment data, etc)?

No, there are not. Data retention *obligations* are always mandated for a specific purpose (cf. Recital 5 TAD). Outside those cases, the general PDPC framework concerning the processing of personal data on a voluntary basis applies.

47. Are there any statistics on cases where the specific objective of a data access (e.g. the detection of serious crimes or the prevention of specific security threats) could be achieved? Are there any evaluations on the effectiveness of data retention in your country as a whole? If so: please provide the main results of the research.

To the author's best knowledge, no statistics or studies as to the effectiveness of data retention rules have been released. The Garante carried out an extensive investigation on the implementation status of data retention rules. The inquiry revealed a number of minor shortcomings and few serious infringements, which resulted in four *ad hoc* injunctions against individual providers ([doc. web. 1484695, 1484726, 1484758, 1524263]) some of which were also reported to the judicial authority for the purposes of criminal proceedings (see Garante, Annual Report 2009, p. 198-199, available at: http://www.garanteprivacy.it/garante/doc.jsp?ID=1730032)

48. Is there any information available about whether and, where applicable, how communication patterns have changed since data retention has been introduced in your country?

There are currently no studies as to the changes in communication patterns relative to the implementation of the data retention directives.

49. Are there any discussions going on in your country to expand/narrow down the categories of data to be retained, their retention period or their purposes of use?

As mentioned in the reply to question 7, lit. a), Article 3, par. 2, TD provides for that new categories of data (i.e. other than those detailed in Article 3, par. 1, TD) subject to retention obligations can be introduced by way of a Decree (i.e. a regulatory act) adopted either by the President of the Council of Ministers or the Minister for innovation and public administration, in agreement with the Ministers for European Policies, Economic Development, Home affairs, Justice, Treasury and Defence, following consultation of the Garante. To date no such decrees have been adopted and no initiatives to that effect have been announced.

C. National constitutional/legal framework

I. Dimension 1 (State – citizen)

50. Which national fundamental rights protecting privacy, personal data and the secrecy of telecommunications do exist in your country? Are there any other fundamental rights granted to citizens that could be affected by data retention (e.g. freedom of expression and information/freedom of the media, freedom of thought, religion/belief and/or conscience, judiciary basic rights, freedom of profession in cases where the confidentiality of communication is essential etc)? Do the fundamental rights mentioned result from the constitution, from other legal acts or from case-law? Please describe the scope of protection of these fundamental rights. As regards the right to secrecy of telecommunications: Which data are – according to national (constitutional) law1 – considered as telecommunications content? Is it legal under national (constitutional) law to retain this content without a specific reason?

Data retention obligations entail a sensitive balancing exercise between a number of values enshrined in the Italian Constitution (hereafter: "IC"):[2] i) the right of privacy, ii) the right to the protection of personal data; iii) the right to freedom of communications and secrecy thereof; iv) the freedom of expression.

The right of **privacy** is not expressly mentioned in the IC and has emerged mainly as a result of judicial lawmaking.[3] In essence, the right of privacy is an entitlement to protection from interferences into each individual's private sphere. As such, it can be characterized as one of the "inviolable rights of the person" enshrined in Article 2

---

1 In the following, „national (constitutional) law" means any national legal norm that (within the national legal system) is at a level superior than that of any other law (in countries with a written constitution: legal norms at constitutional level).

2 An English language translation is available at: http://www.quirinale.it/qrnw/statico/costituzione/pdf/costituzione_inglese_01.pdf; A German language translation is available at: http://www.quirinale.it/qrnw/statico/costituzione/pdf/costituzione_tedesco.pdf)

3 *See, e.g.*, Court of Cassation, judgment no. 2199/1975.

IC. Others have argued that the right of privacy is also underpinned by other IC provisions, such as Articles 14 and 15 (proclaiming the inviolability of private dwellings and correspondence)[4], and Article 13 (on the inviolability of personal freedom). The Constitutional Court, in turn, held that the right of privacy is a corollary of the "equal social dignity" all citizens are entitled pursuant to Article 3(1) IC[5].

The **right to the protection of personal data** consists in every individual's entitlement that his or her personal data be processed by third parties according to requirements and standards set by the law, so that he or she can effectively control the data concerning him or her and can determine the limits and conditions of their processing[6]. That right is expressly recognized in Article 1 PDPC and can be regarded as enjoying the same constitutional status as the right of privacy.

The **freedom of expression** is enshrined in Article 21 IC, whereby everyone has the right to freely express his or her thoughts in speech, writing, or any other form of communication. Limits on that right can only be imposed as a result of a court order, in cases predetermined by the law.

The right to **freedom and confidentiality of communications** is set out in Article 15 IC. Its two components (freedom and confidentiality), albeit intertwined, are subject to different rules in case of non-compliance. With reference to telephone conversations, the Constitutional Court has held that confidentiality must be ensured not only as to the contents of the communication, but also with reference to external features thereof, such as the identity of the participants, as well as the time and place of the conversation.[7]

In the absence of an express legal definition, the notion of '**contents of communications**' can be inferred *a contrario* from the definition of traffic data, which are those strictly necessary to the transmission of the communication and its billing. The degree of ambiguity characterizing the notion at issue have given rise to uncertainties especially in the case of internet communications, where apparently neutral data could in fact reveal essential elements of the content of those communications, thus disclosing sensitive information about the individuals concerned and increasing the risk of profiling.[8] It is worth reminding that the contents of communications cannot be retained (Article 132, par. 1, PDPC).

---

4 M. CUNIBERTI, *Riservatezza e identità personale*, in AA.VV., Percorsi di diritto dell'informazione, Giappichelli Editore, Torino, 2006, p. 123.

5 Corte Cost. sent. 2129/1975.

6 M. GAMBINI, *Dati personali ed internet*, ESI, Napoli, 2008, p. 20 ss.

7 AA.VV., *Commentario alla Costituzione*, Vol. I, art. 15, Utet, Milano, 2006, p. 362 ss.

8 M. GAMBINI, *Dati personali ed internet*, ESI, Napoli, 2008, p. 51 ss.

51. Under which conditions is it permitted to limit the exercise of the fundamental rights mentioned in your answer to question 50, according to national (constitutional) law?

The right to privacy and to the protection of personal data can only be limited to pursue other constitutional values of equal importance, in accordance with the rule of reason and the principle of proportionality and as long as the essential content of those rights is not nullified.[9]. As to the freedom of expression and the right to the freedom and confidentiality of communication, the IC itself provides for that limits can be imposed only by the law and in the presence of a reasoned court order.

52. If national (constitutional) jurisprudence has already ruled on the constitutionality/legality of the legal act(s) transposing the Directive: To which conclusion has it come? Is it possible, according to the court's opinion, to transpose the Directive in conformity with national (constitutional) law?

As mentioned above, courts have not yet ruled on the constitutionality or legality of the TD or of the TAD. It must be recalled, however, that the Italian Constitutional Court, in its judgment no. 372 of 14 November 2006, held that Article 132 PDPC, prior to its amendment by the TD, struck a "fair balance" between the individual right to privacy and the common interest to the suppression of serious crimes.

53. Does national (constitutional) law safeguard an absolute limit as to the maximum degree to which public surveillance measures collectively may restrict fundamental rights, or has an assessment/balance of interests to be carried out in each individual case?

Constitutional law sets out both absolute and relative limits to the restriction of fundamental rights. The former, first and foremost, concern the so called '*diritti indisponibili*', i.e. rights that are so important as to escape any possibility of being balanced against other constitutional values. Apart from those values, other constitutional rights might be subject to a balancing exercise often resulting in relative limits to those rights. As a further absolute limit, however, said balancing exercise cannot restrict one of the values concern so as to deprive it of its essential content. The Constitutional Court was called on a number of times to strike a balance between conflicting interest in the field of privacy and communications[10].

54. Does national (constitutional) law require that exemptions be provided for from the obligation to retain or to transmit certain data that are worth being protected (cf. question 12)?

Other than the freedom of correspondence set out in Article 15 of the Italian Constitution, the Italian Constitution does not expressly require the legislature to lay down exemptions from the obligation to retain or to transmit data. It must be noted,

---

9 Cf. Article 3 PDPC.

10 *See, e.g.*, Constitutional Court judgments no. 9/1965; no. 120/1968; no. 38/1973; no. 11/1974; no. 106/1974; no. 123/1976; no. 16/1981.

however, that courts have drawn support to safeguard the right to privacy from other constitutional provisions, such as the duty to respect fundamental human rights set out in Article 2 and the principle of equality laid down in Article 3.

II. Dimension 2 (State – economy)

55. Does the retention obligation restrict any fundamental right (e.g. professional freedom) protected by national (constitutional) law vis-à-vis the obligated parties (telecommunications and internet service providers etc)? In your opinion (based on/supported by the current state of the discussion in academia and jurisdiction, where available), are these restrictions in line with national (constitutional) law? Where are the limits to such restrictions according to national (constitutional) law?

Retention obligations may be regarded as *prima facie* violations of at least two constitutional values: the freedom of enterprise (enshrined in Article 41 IC) and the right to property (set out in Article 42 IC).

As to the **freedom of enterprise**, the strongest argument for a case of *prima facie* violation would be the non-negligible costs undertakings are required to bear in order to comply with the technical arrangements laid down in the TAD. The economic impact on the freedom of enterprise is all the more apparent in the case of small and medium-sized firms. Moreover, compliance obligations are not an one-off burden, but are likely to entail repeated overhaul and update of the undertakings' systems to such new requirements as the Garante may introduce in the future.

Nonetheless, if a similar claim were ever submitted to the Italian Constitutional Court, the latter would in all likelihood dismiss it at the level of justifications. Article 41 IC, indeed, expressly states that private economic enterprise cannot not be carried out *against the common good* or in such a manner that could damage *safety, liberty and human dignity*. Moreover, Article 41 entrusts the legislature with the task of devising appropriate programmes and controls so that economic activity may be oriented and co-ordinated *for social purposes*. The crime detection and suppression goals underlying data retention obligations can easily fit into one of those pigeonholes, insofar as: i) it carried out in the common good, ii) it pursues the protection of safety, liberty, and human dignity of crime victims, and iii) it is aims at broader social purposes.

It would be naive to make predictions as to the outcome of the judicial application of the Italian rule of reason doctrine (*principio di ragionevolezza*) to a similar case. Nonetheless, it is fair to say that, albeit costly, the economic sacrifices imposed on undertakings are not so significant as to deprive the freedom of enterprise of its essential content. Moreover, in the case of small and medium-sized undertakings, the Garante expressly called for incentive schemes. The proportionality issue would be a close one, but the deference the Constitutional Court has traditionally displayed *vis-à-vis* the legislature's discretion in politically-sensitive matters and its earlier holdings on similar cases[11] (which, albeit not binding on the Constitutional Court,

[11] *See, e.g.*, Constitutional Court Judgment no. 372 of 14 November 2006

have not yet been overruled or distinguished) suggest that, on balance, the constitutionality of the data retention obligations would be upheld.

Turning to the right of property, it is beyond question that, to the extent that databases can be regarded as immaterial property, they fall within the scope of Article 42 IC. Since data retention obligations directly interfere with the database holder's freedom to manage and dispose of its property, a *prima facie* case is yet again warranted. As in the case of the freedom of enterprise, however, a similar case would probably be dismissed at the stage of justifications. Article 42 IC, indeed, expressly entrusts the legislature with the task of ensuring the „social function" of property, a category that would certainly include the public policy goals underlying data retention obligations. Again, the right of property would not be deprived of its essential contents and its restriction by the data retention obligation would be probably regarded as not being disproportionate to the aims pursued.

56. To what extent and under which conditions does national law allow to draw on private actors for the purpose of law enforcement or any of the other purposes of data retention (as far as provided for by the national law transposing the Directive, cf. question 11)?

Rather than specific obligations to assist law enforcement agencies, Italian law provides for general criminal sanctions for *not* providing the necessary assistance (cf. Article 349 Criminal Code, providing for imprisonment up to four years) or for withholding relevant information (e.g. Article 371 bis Criminal Code, providing for imprisonment up to four years).

As a rule, private actors have no law enforcement duties or powers. There are some exceptions (e.g. the individual's power of arrest *in flagrante delicto*) none of which, however, concerns the matter of data retention.

57. According to national (constitutional) law, is it imperative to provide for reimbursement of the obligated parties for the costs incurred?

No, it is not. National laws and regulations do not provide for any reimbursement obligation for the costs incurred in the context of data retention.

III. Dimension 3 (State – State)

58. What status do international treaties and, in particular, the European Convention on Human Rights (ECHR) have within the hierarchy of norms of your country's legal system?

As per Article 10 IC, the Italian legal system conforms to the generally recognised principles of international law. International treaties, instead, come to the fore in the context of Article 117(1), whereby the legislature is required to act „in accordance with. . . Italy's international obligations". Therefore, if a conflict arises between a legislative act and national provisions adopted pursuant to an international agreement, the former can be struck down by the Constitutional Court as incompatible with Article 117(1) IC.

As to the relationship between international law and IC provisions, the Constitutional Court usually endeavours to reconcile potential conflicts by interpreting IC provisions „in the light of" international obligations.[12]

The issue of normative conflicts between national legislation and ECHR provisions has been recently addressed by the Constitutional Court in judgments nos. 348 and 349 of 2007. In those two landmark judgments, the Court essentially held that ECHR provisions have no direct effect, as in the case of EU law provisions. Accordingly, conflicts must be resolved by courts by construing national provisions in the light of ECHR obligations. If that proves unfeasible, then courts may refer the matter to the Constitutional Court which, if the matter cannot be settled by recourse to interpretation in the light of the ECHR, can strike down those provisions as unconstitutional.

59. Are there any situations/configurations that might concede to Directives a particular status within the hierarchy of norms of your country's legal system and/or grant them immediate effect? In general, what steps have to be followed in order to transpose a Directive into national law in your country?

As to the effects of directives in the Italian legal order, there are no significant deviations from the holdings of the Court of Justice on that matter. As a rule, directives require transposition measures in order to be effective in the Italian legal order. Nonetheless, if the transposition deadline has fallen due and some provisions of the directive are clear, sufficiently precise, and unconditional, they can have direct effect, i.e. they can be relied upon by individuals and firms before courts and administrative agencies, subject to the limits of reverse administrative direct effect and horizontal direct effect.

Albeit not compelled to do so by EU law, the Constitutional Court also devised a solution to solve conflicts between legislative acts and EU directive provisions *not* having direct effect. In those cases, if the antinomy cannot be resolved by recourse to consistent interpretation, courts must refer the matter to the Constitutional Court which can strike down the relevant national legislative instrument as unconstitutional. This mechanism proved quite effective in securing consistency of Italian legislation with EU law and thus to forestall possible infringement procedures and non-contractual liability claims by individuals as per the ECJ *Francovich* doctrine.

The transposition of directives is governed by the principles set out in Law no. 11 of 2005: by 31 January of each year, the Government submits a bill to the Parliament setting out the necessary transposition or implementation arrangements to ensure compliance with EU law. As in the case of the Data Retention Directive, this bill often contains enabling provisions that empower the Government to adopt a decree to transpose directives.

---

12 AA.VV., *Commentario alla Costituzione*, Vol. I, art. 15, Utet, Milano, 2006, p. 248 ss.

60. Does national (constitutional) law limit the possibility of your country to transfer national sovereignties to the European Union, or does it limit the possibility for the EU to exercise competence already transferred in cases where this would be in conflict with national (constitutional) law?

As per Article 11 IC, Italy agrees, on conditions of equality with other States, to the limitations of sovereignty that may be necessary to a world order ensuring peace and justice among the Nations. Albeit the drafters of the IC introduced that provisions to ensure the effectiveness of measures adopted by the UN, the Constitutional Court has consistently relied on Article 11 IC to account for the limitations of sovereignty resulting from Italy's membership in the EU.

The Constitutional Court, however, cautioned that the Italian legal order "does not open up unconditionally" to EU law, but only so long as the latter does not exceed certain limits (the so-called "*controlimiti"*), such as the fundamental principles of the Italian legal order and the inviolable rights of the person (see Constitutional Court judgments no. 183 of 1973 , no. 232 of 1989 and 168/1991), as in that event the Constitutional Court would be compelled to review the constitutionality of the Italian law ratifying the EU Treaties.

61. In which way have the powers regarding data retention been divided among ministries and authorities in your country? In case there are regional territorial entities (covering only parts of the country) that are vested with own powers and authorities (cf. question 32): how is competence split among the authorities of these entities and between these authorities and the authorities of the central state/federal state?

As discussed in greater detail in the answer to question 7(a), the legislature enacted legislative transposition measures empowering the Garante to implement them at the regulatory level and to enforce them in case of non-compliance. As per Article 3, par. 2, TD data retention obligations can be extended to new categories of data (i.e. other than those detailed in Article 3, par. 1, TD) by way of a Decree adopted either by the President of the Council of Ministers or the Minister for Innovation and Public Administration, in agreement with the Ministers for European Policies, Economic Development, Home affairs, Justice, Treasury and Defence, following consultation with the *Garante.*

The (internal) division of tasks between the Council of Ministers and individual Ministers (including the President of the Council of Ministers, i.e. the Italian Premier) is governed by law 23 august 1988, no. 400, available (only in Italian) at: http://www.comune.jesi.an.it/MV/leggi/l400-88.htm. It must be noted, however, that the special procedure laid down in the TD supersedes the general procedure set out in law 1988/400 according to the principle *lex specialis derogat generali.*

62. Does national (constitutional) law set any limits regarding the transmission of retained data to other countries? If so: Please describe these limits.

The IC constitution does not deal with the transfer of retained data to other

countries, thus the relevant provisions are those set out in the PDPC and illustrated in greater detail in the reply to question no. 34. The IC, however, does establish some overarching requirements, which also apply to the matter at hand, such as the right of defence (Article 24 IC). As a consequence, the said PDPC provisions must be interpreted in keeping with those requirements.

IV. Assessment of the overall situation

63. In your view, what options for improvement are there in your country in terms of balancing the interests of freedom and security in the context of data retention?

Having regard to the data retention rules in Italy as a whole, two patterns can be clearly discerned: some shortcomings at the legislative level and an ensuing compliance deficit at the regulatory one.

As to the first aspect, the legislature clearly failed to grasp the opportunity offered by the directive to lay down a comprehensive and consistent legislative framework in the matter at hand. In contrast, the TD contains a number of cosmetic changes to the existing PDPC provisions, whose drafting was – and still is – no paragon of legal clarity. Rather than striking a careful balancing exercise between freedom and security in the context of data retention, it appears that the main goal of the legislature was to secure formal compliance with its EU obligations (the first transposition deadline had already fallen due).

As to the second issue, the shortcomings at the legislative level prompted the Garante to act *de facto* as a surrogate lawmaker. The Garante, thus, ended up bearing a substantial regulatory burden at the expense of its enforcement responsibilities. This resulted in a generalized compliance deficit, that compelled the Garante to defer its implementation deadline twice, with adverse consequences on the credibility of the Garante's subsequent enforcement campaign.

In spite of those criticalities, the new rules on data retention undoubtedly constitute an improvement relative to the pre-existing framework, which featured some of the longest data retention periods in the EU.

Turning to the issue of improvements, past legislative practice clearly shows that it is extremely unlikely that the legislature will *motu proprio* revise the data retention legislation in the near future. Refinements, therefore, can credibly only take place at the level of regulation and enforcement. In this connection, the vagueness and ambiguity of the rules at the legislative level could possibly constitute a valuable asset in the hands of the Garante, which enjoys a non-negligible latitude in overhauling the existing regulatory framework.

An area where there is significant room for improvement is the one of process rights of the aggrieved party. It would be commendable to require prior notification to those parties before data concerning them is accessed. Moreover, in keeping with the principles of due process and of *audi alteram partem,* those parties should be involved in the proceedings and should be granted a right to be heard. Admittedly,

the prior notification requirement may, in some cases, prove incompatible with the secrecy needs inherent in pre-trial investigations. However, this also holds true for traditional fact-finding and evidence-gathering operations, such as house and body searches. In those cases, however, the Italian CCP strikes a balance between crime detection and personal liberty by waiving the prior notification requirement but allowing participation in the search of the person subject to investigations and his or her counsel. Arguably, a similar balance can be struck also in the context of data retention obligations.

Balancing the interests in the context of data retention (INVODAS)

Italy

Amedeo Arena

Part 2: Overarching issues and country-specific questions

A. General part (questions to the experts in all Member States)

1. Does national (constitutional) law provide for a right to communicate *anonymously*?

The right to communicate anonymously is an extremely debated legal topic.

Supporters of that right usually regard Article 15 of the Italian Constitution (protecting the freedom and confidentiality of communications) as the constitutional basis for such a right. Indeed, in judgment no. 81/1993, the Constitutional Court squarely held that "the breadth of the protection under Article 15 of the Constitution implies . . . not only the secrecy of the contents, but also of the identity of the subjects between which the communication takes place, as well as the communication's time and place".

Those who are opposed to the recognition of a fully-fledged right to communicate anonymously rely upon the structure of Article 15 of the Constitution, which indeed protects communication "between two or more specific subjects" (see R. Zaccaria and A. Valastro, *Diritto dell'informazione e della comunicazione*, CEDAM: Padua 2010, 88-89). It follows that both the sender(s) and the recipient(s) of a given message must be identifiable, which seems to take anonymous communications outside the scope of Article 15 of the Constitution.

Legislative practice can be taken as another argument against the recognition of a Constitutional right to communicate anonymously. In particular, the so-called "Pisanu Decree" required managers of private circles or public establishments which make terminals enabling connection to the internet available to the general public, as well as to members or customers, to identify the users of those terminals and to retain data as to the hours of use of those terminals, excluding the contents of the relevant communications (see answer to Question 24 in the first questionnaire). It must be noted, however, that those requirements were recently repealed by Decree Law 225 of 2010, converted into Law no. 10 of 2011.

2. **Please illustrate in detail any amendments to current data retention legislation that are presently discussed in your country. How strong (in terms of support they get by the public) are the different arguments uttered in this context? Are the proposals for improvement set out in your answer to question 63 of the first questionnaire discussed in the public? If so: by which parts of society, and what degree of attention do they get in the public debate as a whole? Particularly: is the "quick-freeze" option, as foreseen by the Council of Europe's Cybercrime Convention (Art 16 para. 2), discussed as a potential alternative to data retention?**

   To the author's best knowledge, no amendments to the current data retention legislation involving the 'quick freeze' option are currently being discussed in Parliament.

3. **In which way and to which extent are private actors (citizens, undertakings) generally obligated in your country, by means *other* than data retention, to co-operate with public authorities in the detection, investigation and prosecution of criminal offences and/or for any other of the legitimate purposes for which providers are (also) obligated to retain data?**

   Rather than setting out the specific conduct private actors are required to carry out to cooperate with public authorities in the detection, investigation, and prosecution of crimes, Italian criminal law criminalizes failure to cooperate with the authorities. Article 650 of the Penal Code, in particular, provides that whoever fails to comply with a lawful order by Public authorities for reasons concerning the administration of justice, public policy, public security, or public health is punishable up to three months imprisonment. Moreover, Article 378 of the Penal Code criminalizes the conduct of those who help the author of a crime to elude the investigations of public authorities or to escape capture; Article 379 of the Penal Code punishes helping the author of a crime to acquire the revenue, profit or price of a crime. If one helps a criminal for his or her own interest, that person can be convicted for aiding and abetting in that crime, as per Article 110 of the Penal Code. Finally, as per Article 40, para. 2, of the Penal Code, failing to prevent an event which one was legally required to prevent is tantamount to causing it. The broad scope of the above criminal provisions catches failure to cooperate with the authorities in most of its forms.

4. **Which rules governing the rights of persons (e.g. in specific circumstances such as a lawyer) to refuse to testify/to deliver evidence against themselves (in court) do exist in the national law of your country? Do these rules include (according to their wording or according to the meaning identified through applying commonly used methods of interpretation) data that is to be retained and – as the case may be – transmitted under the national law transposing Directive 2006/24/EC on data retention (hereinafter: "the Directive")? Do these rights to refuse to testify conflict with data retention in a way that they bar these data from being retained, transmitted and/or used as an evidence in court?**

   As per Article 198, paragraph 2, of the Code of Penal Procedure, no witness can be required to testify about facts from which his or her criminal liability may arise. Moreover the defendant can has the right to remain silent and it is well-established that he or she has no obligation to tell the truth (although his or her credibility may be questioned as a result of false statements). As the Code of Penal Procedure was enacted in 1988, the legislature at the time did not contemplate data retention obligations. Neither did the legislature update such provisions when it transposed the data retention directive into national law.

   The matter, therefore, boils down to one of statutory interpretation. The wording of Article 198, paragraph 2, of the Code of Penal Procedure supports a broad interpretation, covering any type of information which could lead to self-incrimination by witnesses or defendants. Moreover, the principle *nemo tenetur se detegere* rests upon the right of defence enshrined in Article 24 of the Constitution. While the legislature can strike a balance between the privilege against self-incrimination and other values of constitutional import, such as the detection and suppression of crimes, such a balancing exercise would in all probability be unreasonable unless expressly regulated by law. It would thus be contrary to the Constitution to construe the said provisions of the Code of Penal Procedure as not including retained data.

5. **Where/how are data, that have been requested by entitled bodies, stored by these bodies once obtained? What measures have to be taken by these bodies in order to safeguard data protection and data security?**

   While the TAD sets out a number of requirements that entities required to retain data must comply with, no rules have been laid down by the legislature or by the Garante concerning the handling of retained data by entities entitled to access that data.

6. **Are there any official statistics or otherwise available information on the transmission of retained data to the entitled bodies (number of requests, data categories, time period between storage and request)? If so: please attach this information or give a brief summary and indicate their source.**

   No, there are no official statistics as to the transmission of retained data to the entitled bodies.

B. Country-specific questions

7. Please give your own opinion on the constitutionality of the data retention regime in your country as a whole.

The data retention regime as a whole may, just as the specific provisions introduced to implement the Directive, be regarded as encroaching upon the freedom of enterprise (Article 41 IC) and the right to property (Article 42 IC).

As to the former, the costs undertakings are required to bear to bring their systems in line with the relevant technical arrangements may be regarded as an obstacle to the pursuit of their freedom of enterprise. Nonetheless, the aims underling data retention (i.e. the detection and suppression of crimes) can be regarded as suitable justifications to such a prima facie violation, insofar as data retention rules are carried out in the common good, pursue the protection of safety, liberty, and human dignity of crime victims and aim at broader social purposes. While it is difficult to foresee the outcome of the balance the Constitutional Court would be required to strike between those conflicting values, the leeway the Court has consistently accorded to the legislature make a finding of compatibility the most probable one.

Since data retention obligations directly interfere with the database holder's freedom to manage and dispose of its property, there is a strong case for a *prima facie* breach of Article 42 IC. The express derogation set out in Article 42 IC for limitations serving a 'social function', however, would undoubtedly apply to the public policy goals underlying data retention obligations. As the right of property would not be deprived of its essential contents, the restriction on that right would be probably regarded as not being disproportionate to the aims pursued.

8. Please describe the Italian Constitutional Court's ruling of 14 November 2006 on the constitutionality of Art. 132 PDPC, as in force prior to the amendments introduced by the TD (plaintiffs/defendants, essential reasons of the ruling, legal consequence). Which elements/aspects did the court consider when trying to strike this balance, and what was the result of such assessments? Please explain the impact of the proportionality rule in this context.

The Constitutional Court, in its judgment no. 372/2006, joined a number of questions of constitutionality concerning different aspects of Article 132 PDPC as amended by Decree-Law 24 December 2003, no. 354. That article was later amended a number of times, thus making the judgment of limited relevance nowadays.

The questions were referred to the Constitutional Court (through a procedure that loosely resembles the preliminary ruling procedure before the ECJ laid down in Article 267 TFEU) by a number of trial criminal courts in the context of cases where the relevant public prosecutor had requested a court order to access telephone traffic data. The name of the defendants are not specified in the judgment.

A number of the questions concerned the third paragraph of Article 132 PDPC, which, in its original version, provided that the public prosecutor had to apply for a

court order to access telephone traffic data less than 24 months old. Some questions concerned the type of assessment that the court had to carry out in deciding whether to grant or deny such an order. Moreover, it appeared incongruous that, while in case of urgency the public prosecutor could order wiretapping of phone conversations (thus accessing the content of those conversation), access to telephone traffic data always required a prior court order, also in cases of urgency.

All of the questions above, however, were dismissed on procedural grounds as the relevant parts of Article 132 PDPC were amended before the Court could render its judgment (*jus superveniens*). The current version of Article 132, paragraph 3, PDPC provides for that the public prosecutor may acquire the relevant data without need for a court order.

The second part of the judgment, instead, concerned the special regime set out in Article 132, para 2, PDPC at the time of the judgment (no longer in force nowadays), for access to telephone traffic *data less than 24-month old* – which was possible for all types of criminal offence – and *access to older data* – which was allowed only for the specific offences listed in Article 407, paragraph 2, letter a) of the Code of Criminal Procedure. Those specific offences included sexual crimes, terrorism-related offences, weapons-related offences, and other serious crimes.

At the outset, the Court clarified that since the legislature had sought to strike a balance between the right of privacy set out in Article 15 IC and the public interest in the suppression of crimes, its task was only to assess whether the legislature had encroached upon any of those two constitutional values in a "manifestly unreasonable manner". The Court also noted that such an assessment must be carried out not in an abstract manner, but having regard to the specific circumstances of the case.

On the merits, the Court held that the balancing exercise carried out by the legislature was not unreasonable, insofar as the greater encroachment upon the right of privacy caused by access to data older than 24 months reflected the greater social concern associated to the specific offences listed in Article 407, paragraph 2, letter a) of the Code of Criminal Procedure.

9. Is the constitutionally fixed limit to a conferral of national sovereignties to the EU, as set out in your answer to question 60 of the first questionnaire, in any way binding for representatives of Italy in EU organs and institutions (e.g. the Council of Ministers, the European Council) when exercising their functions in the adoption and execution of an EU legislative act?

Unlike the *Bundesverfassungsgericht,* the Italian Constitutional Court never went so far as to frame the "controlimiti" doctrine as an *ex ante* constraint on the conduct of Italian representatives in EU organs and institutions. To date, it is fair to say that the Italian Constitutional Court only placed an *ex post* limit on the exercise of the sovereignty transferred to the EU. Should the latter enact legislation that, for instance, encroaches upon the fundamental rights of individuals, the Constitutional Court reserved the right to review compliance of the national statute ratifying the

EU founding treaties with the Italian Constitution. The Constitutional Court, however, has never exercised that power so far.

10. **May access to the data retained be requested for the detection and suppression of *all* criminal offences, or is there a catalogue/definition of criminal offences for the detection and suppression of which access to retained data may be sought? If the latter: please provide this list/definition.**

    As clarified in the answer to question no. 9 above, Article 132 PDPC as amended by Decree-Law 24 December 2003, no. 354 set out, in paragraph 1, a general data retention regime "for the detection and suppression of crimes" and, in paragraph 2, a special data retention regime for specific offences listed in Article 407, paragraph 2, letter a) of the Code of Criminal Procedure. The special regime involved, in particular, the obligation to retain data for a longer period.

    Legislative Decree 30 May 2008, no. 109 repealed paragraph 2 of Article 132, thus abolishing the special regime and the reference to Article 407, paragraph 2, letter a) of the Code of Criminal Procedure. The current version of the PDPC, therefore, requires the retention of telephone traffic data and internet traffic data (respectively for 24 and 12 months) "for the detection and suppression of crimes" in general. That data can only be accessed if the public prosecutor issues a reasoned order.

    The only surviving differential regime for serious crimes is currently set out in Article 132, paragraph 4-ter, PDPC, according to which law enforcement agencies may require providers to retain internet traffic data (excluding contents) up to 90 days (which can be extended up to six months), if necessary subject to specific storage arrangements. Providers must comply with retention orders at once and must keep that order and the ensuing investigations confidential. Retention orders must be notified to the public prosecutor within 48 hours. If the public prosecutor does not endorse those orders, they become ineffective.

11. **As regards your answer to question 30 of the first questionnaire: does *criminal law* provide for any sanctions if data that is to be retained under the TD is handled wrongfully, e.g. used for other purposes? If so, please specify the relevant elements of the criminal offence.**

    As per Article 162-bis PDPC, violations of the PDPC provisions as amended by the TD are punishable by an administrative fine ranging from Euro 10,000 to 50,000, unless the facts at issue constitute a criminal offence.

    Article 5, par. 2, TD further provides for that the allocation of an IP address unable to univocally identify the user is punishable by an administrative fine ranging from Euro 5,000 to 50,000, which can be tripled in relation to the economic conditions of the subject. The Ministry for Economic Development is responsible for the establishment of infringements and the application of those sanctions (subject to judicial review by courts).

Moreover, as mentioned in the reply to question 20, damages suffered as a consequence of the violation of data retention provision can give rise to a civil action as per Article 2050 of the Civil Code.

12. **Are there any rules preventing the same data from being retained more than once (e.g. when the network operator and the service provider are different legal personalities who, in principle, would both be covered by the retention obligation)? From your answer to question 23 of the first questionnaire, I understand that such a rule might be derived from Recital no. 3 TAD, according to which only service providers are obligated to retain traffic and location data, but not the operators of the networks used for the provision of such services. Does Recital 3 TAD have binding effect, or is this just an interpretation rule?**

Most regrettably, the PDPC is rather unclear as to the addressees of its data retention obligations. It is for that reason that the TAD devoted a whole recital to the issue, in an attempt to clarify the relevant PDPC provisions.

The legal status of Recital 3 of the TAD is, however, uncertain, as the provision of recitals preceding the substantive content of an act is rather unusual in Italian law. Still, TAD's legal basis, i.e. Article 132(5) PDPC, expressly empowers the Garante to lay down technical arrangements and measures designed to protect personal data, not to define or clarify the subjective scope of other PDPC provisions, such as the one set out in Article 132, paragraph 1 and 1-bis. Therefore, the Garante would be acting *ultra vires* if it sought to rely upon its regulatory power under Article 132(5) PDPC to broaden or to narrow the scope of data retention obligations. It follows that, in all likelihood, Recital 3 TAD is a non-binding interpretation guideline.

While providers of electronic communications services (excluding content providers) appear the most obvious candidates for subjection to the data retention obligations, it must be noted that paragraph 1-bis of Article 132 PDPC (concerning unsuccessful calls data) refers to "providers of publicly available electronic communications services *or a public communications network*" (emphasis added). Likewise, Decree-Law 27 July 2005, no. 144 set out transitional arrangements imposing data retention obligations upon providers of *a public communications network* or publicly available electronic communications services". The TAD also provides that "the requirement to retain data applies . . . to the entities that bring into effect . . . the conveyance of signals on electronic communications networks – *irrespective of the proprietary status of such networks* – and offer services to end-users in pursuance of the non-discrimination principle".

13. **Can the differences in the language of Article 132 paragraph 1 and 1-bis be taken as implying that providers of public communication network are only bound by the obligation to retain data related to unsuccessful calls?**

This seems unlikely. While only application by courts and implementation by the Garante will clarify the exact personal scope of data retention provisions, at this juncture it must be noted that the EU doctrine of consistent interpretation requires

that all national provisions, and especially those designed to implement Directive 2006/24/EC, be construed in the light of the aims and content of that Directive.

The latter, in Article 3, paragraphs 1 and 2, makes it sufficiently clear that both 'providers of publicly available electronic communications services' and 'public communications network providers' are subject to the obligation to retain data, including data relating to unsuccessful calls.

14. **While data retention, according to your answer to question 11 of the first questionnaire, is mandated for the purposes of "detecting and suppressing criminal offences" only, the purposes of use of these data seem to be wider: as stated in your answer to question 15 of the first questionnaire, "retained data can be used in order to detect and suppress criminal offences, as well as for the purposes of pre-trial investigations, the prevention of terrorist crimes etc." Can you explain the reasons for this difference? Where in the law can the relevant provisions be found?**

Article 132, para 4-ter PDPC provides that law enforcement agencies (not the public prosecutor, as in the case of Article 132, para 1, PDPC) may require providers to retain traffic data up to 90 days 'In order to carry out the pre-trial investigations envisaged by Article 226 of legislative decree no. 271 of 1989' or 'for the detection and suppression of specific crimes'.

That provision (Article 226 of legislative decree no. 271 of 1989) authorizes wiretapping and monitoring of conversations to gather facts relating to the prevention of certain crimes, including civil war, participation in a organized crime, mass murder etc. It must be noted, however, that information gathered through the pre-trial investigations above, cannot be relied upon as evidence in court (neither directly, nor through testimony), but can only be use for investigation purposes.

It is thus fair to say that the only legitimate purpose of data retention is, as clarified in Recital 5 TAD, the detection and suppression of crimes. The reference to certain specified crimes does not broaden the scope of legitimate aims, rather it allows law enforcement agencies to require providers to retain data directly, subject to *ex post* control by the public prosecutor, in order to detect those crimes.

15. **Does Italian law provide for rules on the transfer of personal data to third countries that correctly transpose the provisions laid down in Chapter IV of Directive 95/46/EC? Please describe the content of such rules.**

The provisions laid down in Chapter IV of Directive 95/46/EC (in this answer: the Directive), dealing with cross-border data flows to third countries, have as their national counterparts the provisions set out in Title VII of the PDPC, notably articles 43-45.

Article 45 sets out a general prohibition to transfer personal data to third countries whose legislation does not ensure an adequate level of protection for individuals. This provision loosely reflects the principle enshrined in Article 25.1 of the Directive.

Article 44(1)(b) allows transfer of personal data to third countries whose protection level has been regarded as adequate by the European Commission under Articles 25(6) and 26(4) of the Directive. For instance, in its decision of 3 February 2011, no. 47 (OJ Italian Republic 23 February 2011, no. 44) the Garante authorized the transfer of data to Andorra, following Decision 2010/625/EU (OJ European Union L277/27 21 October 2010) stating that such country offered an adequate level of protection for data transferred from the EU.

Under Article 44(1)(a), the Garante may authorize data transfer to third countries if it deems that the level of protection of personal data is adequate, also in connection with contractual safeguards. This provision was apparently designed to implement the exception clause set out in Article 26(2) of the Directive. For instance, in its Decision of 27 May 2010, no. 46294 (OJIR 19 June 2010, no. 141) the Garante authorized the transfer or personal data to third countries carried out in accordance with certain model contract clauses listed in the attachment to the European Commission's Decision 2010/87/EU (OJEU L 39/5 12 February 2010).

Article 43 enables the transfer of data to third countries subject to a number of requirements, most of which reflect the ones set out in Article 26(1), letters (a) to (f) of the Directive. Please refer to the English language version of the PDPC for the text of those requirements.

16. **Please describe the rules for co-operation among the different bodies accessing the data and between these and other public authorities in detail, as far as they apply to the exchange of these data. In particular, what do the general provisions mentioned in your answer to remark m12/question 33 of the first questionnaire foresee in this respect?**

The existing rules governing co-operation among different public authorities provide nothing in respect of data retention. The principle of 'good administration' set out in Article 97 of the Constitution applies to all public administrations and has been interpreted as requiring administrative action to pursue the general interest impinging as little as possible on private interests. Law no. 241/1990 also sets out general principles governing administrative procedures, including cost-effectiveness, efficiency, impartiality, publicity, and transparency. It also lays down some general rules concerning co-operation in the context of procedures involving more than one administration (articles 14 ff.). Still, none of those provisions appear to be relevant to the topic of data retention.

17. **As regards your answer to question 34 of the first questionnaire, (cross-border co-operation in data retention issues): Please add information about which bodies are responsible for handling cross-border data exchange with regard to the data retained under the TD (in and outgoing requests). May data be accessed directly by the entitled bodies?**

Neither the TD nor the TAD lay down arrangements concerning the handling of cross-border data other than those referred to in the answer to Article 34 of the first questionnaire. By the same token, the Garante has not yet ruled on that issue.

18. Which public bodies are responsible for supervising *that the bodies entitled to obtain access to the data retained* (police etc) act within the law? Are these bodies independent in the sense of what has been said in question 35 of the first questionnaire?

There are no specific rules concerning the supervision of the bodies entitled to obtain access to retain data. Therefore, the ordinary supervision framework applies. In particular, most law enforcement agencies are part of the Ministry of Home Affairs. When they are acting in the course of judicial proceedings, however, law enforcement agencies are accountable to the Deputy Public Prosecutor in charge of the investigation. Deputy Public Prosecutors are members of the Italian judiciary and as such they are independent from the executive branch. They are only coordinated by a Prosecutor-in-chief who, in exceptional circumstances, may take investigations into his or her own hands.

Update on the Data Retention Regulation in Italy

Interception of Communications by Judicial Authorities: Enhanced Security Measures To Be Implemented

The Italian Data Protection Authority has set out measures and arrangements public prosecutor's offices in Italy will have to implement in order to enhance the security of any personal data they collect and use as part of intercepted communications.

The Decision by the Italian DPA (web doc. No. 2551507) followed a fact-finding survey the DPA had started last year on a sample of medium-sized public prosecutor's offices in Italy (Bologna, Catanzaro, Perugia, Potenza, Venice). The survey was aimed to assess the technological and organizational measures that were applied by those judicial offices when carrying out telephone wiretapping or the interception of Internet and electronic communications. Security measures had been already imposed on the electronic communications service providers that forward intercepted data to the judicial authorities requesting such data.

The findings of the survey showed a medley patchwork of situations, which made it necessary to step in so as to enhance the security of both data and data management systems by applying the relevant measures to all public prosecutor's offices; in this manner, data protection measures would be harmonized also in the light of the continuously evolving electronic communications technologies as well as of the possible risks arising from the use of IT tools.

"It is especially important to protect the personal information that is collected and used as part of intercepted communications because of the effects the misuse of such information may produce both on the dignity and rights of the intercepted individuals and of any individuals communicating with them and on the expected effectiveness of the investigation", said Mr. Antonello Soro, President of the Italian DPA.

Accordingly, the Italian DPA required public prosecutor's offices to implement several stringent measures within 18 months as of publication of its decision in Italy's Official Journal [Gazzetta Ufficiale]. The measures in question concern both the "Telecommunications Interception Centres" [Centri Intercettazioni Telecomunicazioni, CIT) operating at each public prosecutor's office and the police offices tasked by judicial authorities with performing interceptions.

Physical Security Measures

In order to access the listening rooms at public prosecutor's offices, the premises hosting the servers where intercepted telephone or Internet communications are stored or the premises hosting the receiver equipment of such communications, individually allocated badges associated with a numerical code (only known to the individual data subject) or biometrics-based devices will have to be used. All accesses will have to be logged. The technical staff in charge of maintenance or technical interventions will have to be authorized beforehand by the individual public prosecutor's office. Such technical staff

will only be allowed to access the data, information and records that are absolutely necessary for their maintenance activities. CCTV cameras will have to be in operation.

IT Security Measures

The systems and servers used for interception activities will only be accessed by operators (including system administrators) from dedicated workstations on the basis of strong authentication procedures. Such workstations will have to be connected with firewall-protected networks.

All the operations performed as part of interception activities – such as listening, browsing, recording, duplicating and storing information, making transcripts of intercepted communications, maintenancing of systems, destroying records and media – will have to be logged via IT techniques that can ensure non-alterability of such logs.

Mastering and duplication of intercepted contents may only be performed where indispensable by duly authorized staff. Records copied to removable media (e.g. CD-ROMs) will have to be protected via encryption. Containers or envelopes used to carry such media may not bear any information that can allow unauthorised third parties to infer or deduce the scope of the interception.

Only judicial police staff may be relied upon to deliver media and paper records (including transcripts) to judicial authorities.

Soundtracks, any other type of collected information and backup copies will have to be stored in encrypted format. Data extraction may only be performed by way of cryptographic procedures.

All data will be exchanged between judicial authorities and Internet service providers via secure network protocols in encrypted format. The intercepted electronic communications – IP-address flows, e-mails – will have to be transmitted from the interception access point on the provider's network to the receiver equipment at a CIT in encrypted format as well.

"Roaming" of Interceptions

As regards the so-called "roaming" of interceptions - i.e. the re-routing of intercepted communication flows from the CITs at public prosecutor's offices to the judicial police offices tasked with such interceptions - the physical and IT security measures to be deployed in the premises used for listening to and recording such flows will have to be the same as those applying to CITs.

The links between public prosecutor's offices and the relevant police offices will consist in dedicated "point-to-point" connections or else be based on secure networks (e.g. VPNs).

Finally, the Italian DPA drew the Ministry of Justice's attention to the need for making available the necessary resources in order for public prosecutor's offices to fully implement the measures set forth in its decision – which "is part of a broader exercise to

enhance security of citizens' personal data vis-à-vis all public administrative bodies", as recalled by Mr. Soro.