QUESTIONNAIRE ON IMPLEMENTATION OF DIRECTIVE 2006/24/EC

Question 3 A:

The Italian DPA is competent for any processing operation that falls within the scope of application of the Community directives mentioned above; indeed, failing different provisions, the general rules set forth in the DP Code apply, whereby the Italian DPA is competent for the processing of personal data under the terms of Section 5 of the Code.

Traffic data retention is regulated specifically by section 132 of the DP Code, which was amended recently by decree no. 109/2008 transposing the data retention directive into Italian law.

Section 4 of legislative decree no. 109/2008 requires service providers to send the Ministry of Justice, by the 30th of June of each year, statistical information that will have to be forwarded to the European Commission.

Accordingly, the statistical information in question is only sent to the Ministry and does not reach the Italian DPA.

It would actually be appropriate for that information to be also sent to our DPA, being the national supervisory authority for personal data protection.

It should be pointed out that under section 3(2) of decree no. 109/2008 the Italian DPA should be consulted in the process leading to the adoption of the Ministerial decree where the data to be retained will have to be specified, if this proves necessary to also take account of technological developments with regard to the data categories mentioned in decree 109/2008. The Ministerial decree in question (which might also be issued by the Prime Minister’s Office) is to be adopted in agreement with other Ministries (European policies, economic development, home affairs, justice, economy and finance, defence).
Question 3 A 1:

Yes. The Italian DPA has carefully followed up on the issues related to the retention of telephone and Internet traffic data, partly via ad-hoc in-depth inspections carried out in respect of the main providers of electronic communications services (including fixed and mobile telephony).

Compliance with the legislation and regulations transposing directive 2006/24/EC – i.e. decree no. 109/2008 and the Italian DPA’s decision dated 17 January 2008 as supplemented by another decision dated 24 July 2008 – will be assessed by our DPA after 15 December 2009; this is the deadline by which providers are required to implement the security measures for traffic data set forth, in particular, via the DPA’s decisions mentioned above. At all events, five inspections were performed in September and October this year following several claims and reports as well as in connection with an enforcement action detailed below; those inspections concerned providers of electronic communications services, and in three of them specific injunction orders and sanctions were issued because of non-compliance with the general legislation on traffic data retention (retention period; data categories).

In particular, the claims and complaints in question had to do with the security measures for accessing traffic data and the allegedly unlawful processing operations performed by employees and/or co-workers of the service providers considered.

It should be recalled that the Italian DPA is actively contributing to the WP29’s work, in particular the joint enforcement action involving national DPAs. The questionnaire developed jointly by the DPAs was administered to service providers, whilst on-the-spot inspections are in progress; the relevant findings are expected by the Spring of 2010.

Question 3 A 2:
Yes. The powers vested in the Italian DPA translate into several activities (imposition of sanctions; issuance of decisions and/or injunction orders and/or prohibitions; performance of inspections; etc.) as also related to public bodies/authorities, providing the personal data protection Code applies (see section 5 thereof).

No complaints and/or claims have been lodged so far by public authorities in their capacity as users of service providers. On the other hand, it should be recalled that neither directive 2002/58 nor directive 2006/24 applies to closed communication networks, which make up the majority of the networks managed by public bodies. Hence, no information can be provided in this connection.

**Question 3 A 3:**

The Italian DPA is empowered to check that providers comply with the directive both via ad-hoc requests for information following complaints/reports lodged with the DPA and by means of on-the-spot inspections at the providers’ premises.

Inspections were performed in 2007 with regard to major providers of telephone and Internet services in order to assess compliance with the requirements the DPA had set forth in a decision dated 15 December 2005, which concerned the interception of telephone and Internet communications; such inspections highlighted cases in which information on the users’ Internet navigation (visited web sites) had been retained unlawfully along with other cases where inappropriate security measures had been implemented to protect personal data retained for law enforcement purposes. Regarding the violations in question, the Italian DPA ordered erasure of the data retained unlawfully as well as the adoption of specific technical measures to secure the personal data at issue; this was done by way of individual, targeted decisions issued in January 2008.
During the inspections carried out in 2009 as part of the enforcement action promoted by the WP29, the Italian DPA found that the companies considered were basically compliant with the applicable provisions. However, some irregularities could be pinpointed, which made it necessary for the DPA to issue injunctive orders and/or prohibitions against three of the companies in question (dated 21 October and 19 November 2009, respectively); furthermore, various sanctions were notified for as many breaches of the legislation on personal data protection (e.g. because the retention period was in excess of the one provided for by law; the minimum security measures had not been adopted; or the ad-hoc security measures imposed by the DPA had not been implemented).

The said inspections also showed that providers resorted increasingly to outsourcing agreements in respect of several operations related to traffic data retention. However, the roles and functions to be allocated to the individual stakeholders pursuant to data protection legislation did not prove to be always clearly determined and specified – with particular regard to the appointment of data processors and the persons in charge for the processing.

**Question 3 A 4:**

The problems encountered so far have to do mostly with practices. Based on the legislation previously in force, Italian service providers used to retain traffic data for long periods, indeed for longer than is currently the case, in order to be able to hand over the data to the judiciary upon request. It should also be pointed out that the scope of the traffic data was broader than the one set forth in the directive.
Furthermore, the mechanisms implemented in providing the services, e.g. via outsourcing, resulted (and still result) into processing operations performed by entities outside national borders – which hampered (and still hampers) application of the national DP Code as well as effective supervision by our DPA.

**Question 3 A 5:**

As for the issues related to centralised databases, special importance should be attached to the mechanisms for applying the Italian – and European – legislation to the processing operations performed by major providers that are established outside the EU, in particular in the US (such as Google and Yahoo!). The DPA is currently analysing the various services made available by the said providers to determine the relevant data protection issues, establish whether connecting links can be found between the said processing operations and our legal system, and decide on the policy to be followed (e.g. implementing moral suasion actions; issuing injunctive orders and/or prohibitions; imposing sanctions, etc.).

Additionally, in-depth inquiries concerning data retention activities for law enforcement purposes, which also addressed technical issues, along with the inspections mentioned under 3A3 led the Italian DPA to set forth the fundamental rules for securing telephone and Internet traffic data that is retained for preventing and suppressing criminal offences – partly on the basis of the information gathered via a public consultation that had been launched on 19 September 2007. More specifically, a decision dated 17 January 2008 concerning the security of telephone and Internet traffic data laid down requirements that can be applied – at least with regard to the general underpinning principles – to centralised databases containing traffic data as well. Such requirements include, in particular, the following: data access mechanisms; regulated
access to premises; authorisation systems; logging of the activities performed by the personnel in charge; separate retention of the data intended exclusively for the prevention and suppression of criminal offences; data erasure mechanisms; regular internal controls; deployment of encryption systems (the said decision is available at www.garanteprivacy.it/garante/doc.jsp?ID=1502599).

The Italian DPA has ordered some of the above requirements to be also applied to the retention of data for purposes of billing, marketing of services, statistics, etc. so as to ensure the security of data and systems in a broader perspective. Conversely, certain controllers fall outside the scope of application of the said requirements, both because they may not be equated to providers of electronic communications services and because of the need for preventing unjustified data retention; such controllers include the managers of shops and Internet cafés, content providers, search engines, and public administrative bodies and companies that make available internal (in-house) telephone and Internet networks to their employees and/or rely on servers made available by other entities.

Providers were required initially to comply with the above measures by 31 October 2008, however this deadline was partly postponed to 15 December 2009 (via a decision dated 24 July 2008) on account of supervening legislation as well as of the complex implementing mechanisms applying to some measures. The latter deadline also applied to adoption by providers of the measures and arrangements set forth by the DPA via a decision dated 27 November 2008, which addressed the allocation of system administrator functions and was targeted to the controllers of processing operations performed electronically.
The Italian DPA has strived to follow an approach that could adequately reconcile various requirements ranging from corporate organisation to law enforcement, data security, and the right to personal data protection.

**Question 3 A 6:**

Apart from the decisions by our DPA mentioned in the reply to question 3 A 1, there is limited case law directly concerning data retention issues.

Reference can be made to the decision by Italy’s Constitutional Court no. 372 dated 14 November 2006, which ruled that the constitutionality claim related to section 132 of the DP Code, as replaced by section 3 of decree no. 354/2003, was unsubstantiated. Under the provision in question, telephone traffic data were not to be acquired and used for the suppression of offences other than those referred to in section 407(2)a of Italy’s Criminal Procedure Code upon expiry of the 24-month retention period.

The Court of Rome ruled in 2007 (case Peppermint and Techland v. Wind telecomunicazioni SpA; case Peppermint and Techland v. Telecom Italia S.p.A.) – contrary to what it had found initially – that the providers of publicly accessible electronic communications services were not entitled to disclose the user identities corresponding to IP addresses to private entities, since the applicable traffic data retention legislation only allows the information in question to be disclosed to judicial authorities for detecting and suppressing criminal offences (see section 132 of the DP Code).

Reference should also be made to two important decisions by Italy’s Constitutional Court, although they date back to a few years ago (no. 81/1993 and no. 281/1998). The Court drew a clear-cut distinction between the interception of communications – which involves processing the contents of communications – and the acquisition of traffic data records – which must not include contents information.
Question 3 B:

Regarding traceability of the users of mobile telephony services as for pre-paid SIM cards, the Italian DPA took steps in respect of specific cases insofar as they were submitted to its attention. Not enough information is available as yet to establish how effective the measures in question have been; they are described in detail below.

Concerning rescue aid, the DPA clarified in a decision dated 19 December 2008 that the Italian DP Code allows a telephone company to notify a rescue body, in real time and without any delay, of data such as the cells activated and/or “engaged” by the missing person’s mobile phone – even without the person’s consent – if this is necessary to safeguard the person’s life and/or integrity. This decision only applies to location data other than traffic data, i.e. the data that can be collected from an electronic communications network irrespective of the existence of a communication between two or more entities.

The above decision concerns Alpine rescue aid, however it lays down principles that are applicable – with some adjustments – to any other type of rescue activity as well. The DPA also clarified that the data acquired by rescue bodies will have to be used exclusively to search and rescue missing persons; it was also recalled that the services enabled to receive emergency calls may process location data related to the caller’s telephone even if the user/subscriber has refused and/or failed to provide his/her consent (see recital 36 and Article 10(1)b. of directive 2002/58/EC and section 127(4) of the Italian DP Code).

As for the incoming traffic related to pre-paid SIM cards, reference can be made to a decision dated 3 November 2005 whereby the Italian DPA ruled that a subscriber and/or
the holder of a pre-paid SIM card could access the personal data related to incoming telephone traffic – including SMS and MMS traffic – only if it could be proven that the data in question was indispensable to safeguard the subscriber’s/card holder’s rights in connection with criminal proceedings, since failure to do so would actually jeopardize their defence rights in the specific case. The Italian DPA also ordered providers to obtain a statement either directly from the data subject or from the data subject’s counsel (based on a POA) to certify that the information provided is true and that the data will not be used for any other purposes.

Reference should also be made to a decision dated 16 February 2006, in which the Italian DPA required telephone operators to implement procedures that should allow timely detecting the existence of several pre-paid phone cards owned by the same person; this was aimed at countering a practice that was rife in Italy, whereby pre-paid phone cards were allocated to individuals who were unaware thereof. More specifically, telephone operators are now to request the owner’s explicit authorization prior to allocating a pre-paid card if that owner is found to already have 4 (in case the owner is a natural person) or 7 (in case the owner is a legal person) cards at his disposal. Additionally, the Italian DPA required telephone operators, electronic communications providers and call centres to carefully monitor the activities of sales points and agents, also by means of sample controls, to quickly detect wrongdoers.

In this connection, it should also be recalled that specific inspections are in progress to investigate this issue, partly in co-operation with the Italian Financial Police (Guardia di Finanza).
QUESTIONNAIRE ON IMPLEMENTATION OF DIRECTIVE

2006/24/EC

- PART II

3 A 3

The Italian DPA is empowered to check that providers comply with the directive both via ad-hoc requests for information following complaints/reports lodged with the DPA and by means of on-the-spot inspections at the providers’ premises.

Inspections were performed in 2007 with regard to major providers of telephone and Internet services in order to assess compliance with the requirements the DPA had set forth in a decision dated 15 December 2005, which concerned the interception of telephone and Internet communications; such inspections highlighted cases in which information on the users’ Internet navigation (visited web sites) had been retained unlawfully along with other cases where inappropriate security measures had been implemented to protect personal data retained for law enforcement purposes. Regarding the violations in question, the Italian DPA ordered erasure of the data retained unlawfully as well as the adoption of specific technical measures to secure the personal data at issue; this was done by way of individual, targeted decisions issued in January 2008.

During the inspections carried out in 2009 as part of the enforcement action promoted by the WP29, the Italian DPA found that the companies considered were basically compliant with the applicable provisions. However, some irregularities could be pinpointed, which made it necessary for the DPA to issue injunctive orders and/or prohibitions against three of the companies in question (dated 21 October and 19 November 2009, respectively); furthermore, various sanctions were notified for as many breaches of the legislation on personal data protection (e.g. because the retention period
was in excess of the one provided for by law; the minimum security measures had not been adopted; or the ad-hoc security measures imposed by the DPA had not been implemented).

The said inspections also showed that providers resorted increasingly to outsourcing agreements in respect of several operations related to traffic data retention. However, the roles and functions to be allocated to the individual stakeholders pursuant to data protection legislation did not prove to be always clearly determined and specified – with particular regard to the appointment of data processors and the persons in charge for the processing.

3 A 5

As for the issues related to centralised databases, special importance should be attached to the mechanisms for applying the Italian – and European – legislation to the processing operations performed by major providers that are established outside the EU, in particular in the US (such as Google and Yahoo!). The DPA is currently analysing the various services made available by the said providers to determine the relevant data protection issues, establish whether connecting links can be found between the said processing operations and our legal system, and decide on the policy to be followed (e.g. implementing moral suasion actions; issuing injunctive orders and/or prohibitions; imposing sanctions, etc.).

Additionally, in-depth inquiries concerning data retention activities for law enforcement purposes, which also addressed technical issues, along with the inspections mentioned under 3A3 led the Italian DPA to set forth the fundamental rules for securing telephone and Internet traffic data that is retained for preventing and suppressing criminal offences – partly on the basis of the information gathered via a public consultation that had been launched on 19 September 2007. More specifically, a decision
dated 17 January 2008 concerning the security of telephone and Internet traffic data laid down requirements that can be applied – at least with regard to the general underpinning principles – to centralised databases containing traffic data as well. Such requirements include, in particular, the following: data access mechanisms; regulated access to premises; authorisation systems; logging of the activities performed by the personnel in charge; separate retention of the data intended exclusively for the prevention and suppression of criminal offences; data erasure mechanisms; regular internal controls; deployment of encryption systems (the said decision is available at www.garanteprivacy.it/garante/doc.jsp?ID=1502599).

The Italian DPA has ordered some of the above requirements to be also applied to the retention of data for purposes of billing, marketing of services, statistics, etc. so as to ensure the security of data and systems in a broader perspective. Conversely, certain controllers fall outside the scope of application of the said requirements, both because they may not be equated to providers of electronic communications services and because of the need for preventing unjustified data retention; such controllers include the managers of shops and Internet cafés, content providers, search engines, and public administrative bodies and companies that make available internal (in-house) telephone and Internet networks to their employees and/or rely on servers made available by other entities.

Providers were required initially to comply with the above measures by 31 October 2008, however this deadline was partly postponed to 15 December 2009 (via a decision dated 24 July 2008) on account of supervening legislation as well as of the complex implementing mechanisms applying to some measures. The latter deadline also applied to adoption by providers of the measures and arrangements set forth by the DPA via a decision dated 27 November 2008, which addressed the allocation of system administrator functions and was targeted to the controllers of processing operations performed electronically.

The Italian DPA has strived to follow an approach that could adequately reconcile various requirements ranging from corporate organisation to law enforcement, data security, and the right to personal data protection.
Regarding traceability of the users of mobile telephony services as for pre-paid SIM cards, the Italian DPA took steps in respect of specific cases insofar as they were submitted to its attention. Not enough information is available as yet to establish how effective the measures in question have been; they are described in detail below.

Concerning rescue aid, the DPA clarified in a decision dated 19 December 2008 that the Italian DP Code allows a telephone company to notify a rescue body, in real time and without any delay, of data such as the cells activated and/or “engaged” by the missing person’s mobile phone – even without the person’s consent – if this is necessary to safeguard the person’s life and/or integrity. This decision only applies to location data other than traffic data, i.e. the data that can be collected from an electronic communications network irrespective of the existence of a communication between two or more entities.

The above decision concerns Alpine rescue aid, however it lays down principles that are applicable – with some adjustments – to any other type of rescue activity as well. The DPA also clarified that the data acquired by rescue bodies will have to be used exclusively to search and rescue missing persons; it was also recalled that the services enabled to receive emergency calls may process location data related to the caller’s telephone even if the user/subscriber has refused and/or failed to provide his/her consent (see recital 36 and Article 10(1)b. of directive 2002/58/EC and section 127(4) of the Italian DP Code).

As for the incoming traffic related to pre-paid SIM cards, reference can be made to a decision dated 3 November 2005 whereby the Italian DPA ruled that a subscriber and/or the holder of a pre-paid SIM card could access the personal data related to incoming telephone traffic – including SMS and MMS traffic – only if it could be proven that the data in question was indispensable to safeguard the subscriber’s/card holder’s rights in connection with criminal proceedings, since failure to do so would actually jeopardize their defence rights in the specific case. The Italian DPA also ordered providers to obtain a statement either directly from the data subject or from the data subject’s counsel (based
on a POA) to certify that the information provided is true and that the data will not be used for any other purposes.

Reference should also be made to a decision dated 16 February 2006, in which the Italian DPA required telephone operators to implement procedures that should allow timely detecting the existence of several pre-paid phone cards owned by the same person; this was aimed at countering a practice that was rife in Italy, whereby pre-paid phone cards were allocated to individuals who were unaware thereof. More specifically, telephone operators are now to request the owner’s explicit authorization prior to allocating a pre-paid card if that owner is found to already have 4 (in case the owner is a natural person) or 7 (in case the owner is a legal person) cards at his disposal. Additionally, the Italian DPA required telephone operators, electronic communications providers and call centres to carefully monitor the activities of sales points and agents, also by means of sample controls, to quickly detect wrongdoers.

In this connection, it should also be recalled that specific inspections are in progress to investigate this issue, partly in co-operation with the Italian Financial Police (Guardia di Finanza).