COMMISSION’S QUESTIONNAIRE WITH A VIEW TO TAKE A STOCK OF THE OPERATION OF ON THE RETENTION OF DATA GENERATED OR PROCESSED IN CONNECTION WITH THE PROVISION OF PUBLICLY AVAILABLE ELECTRONIC COMMUNICATIONS SERVICES OR OF PUBLIC COMMUNICATIONS NETWORKS AND AMENDING DIRECTIVE 2002/58/EC.

Part A:

1. Since July 3rd, 2008 when the EU Directive 2006/CE/24 was endorsed by the Italian government.
2. In Italy legal obligations related to DR are proportional to operator’s business size and type of services. Operators of any size are bound to requirements set forth by the law.
3. Data retained to satisfy legal obligation for criminal prosecution and/or national security is different in terms of details (a lot more detailed) than data processed for billing and fraud fighting purposes. Therefore the whole data retention data warehouse costs, including dedicated security measures, being purposely built to satisfy such legal requirements, are additional to the routine business costs.
4. In order to satisfy at the same time both the data retention requirements and data protection requirements, dedicated and specific security measures were implemented in order to prevent unauthorized access and to carefully log and trace accesses to retained data within the legal framework.
5. Until now, we never received direct requests from any other member states.

Part B:

1. We are not authorized to disclose any information about data served to law enforcement agencies, neither yearly quantity, neither origin of requests.
2. We are not authorized to disclose any information about data served to law enforcement agencies, neither yearly quantity, neither origin of requests.
3. Currently, e.g., telephony data are retained for 24 months. There is a significant difference among LEA requests in terms of time elapsed between the date on which data were retained and the date of LEA’s request, from 10 days to 24 months. However, quite often, especially during investigations against organized crime and/or terrorism, LEAs request data older than the maximum retention period of time, thus leading to the operator to be unable to provide data that have been already purged from data warehouse.
4. Data is sent to the duly authorized requesting agency by means of encrypted message over certified electronic email over public internet.
5. Those identified in the Italian Criminal Procedure Code.
6. We are not authorized to disclose any information about LEAs’ requests for retained data.

Part C:

1. Operators of any size are bound to requirements set forth by the law. Therefore there are no effects of the implementation of the Directive on the domestic competition. However, since the legal obligation are different among EU member states, likely being the italian national requirements more tought than most EU member, the italian telecommunication industry is negatively affected in the competition against most european member states’ industry. The situation is even worse in the competition against non-EU states.

November 09
2. Since most of the new technologies have not been designed with such degree of data logging, binding the DR regulation in place, any new infrastructure design needs to be carefully reconsidered and new services deployments need to be delayed in order to implement data retention functionalities that were not necessary for running the operator’s core business.

3. Given the international competition, in order to preserve our market share, we have no chance to increase the retails rates; hence the only option is to negotiate with LEAs a reasonable cost recovery plan and/or to accept DR costs as losses.

Part D:

1. Data retained are stored in a data warehouse that is located in a single location for the whole network in addition to a secondary disaster recovery site. Data warehouse in both sites are fully owned and managed by the operator.

2. There is no transfer of retained data from our country to/from any other country.