Replies by Hellenic Republic
Ministry of Justice, Transparency and Human Rights
18 12 2009

1.A Qualitative and quantitative aspects of the application of Directive 2006/24/EC, taking into account further developments in electronic communications technology and the statistics provided pursuant to Article 10,

1.A.1 Law enforcement issues

1.A.1.a Total number of requests that are issued by year to obtain data retained under the DRD [Quantitative Reply]

Requests and Orders that are issued, under the current legal framework (not under the DRD because of the non implementation):

a) For the year 2006: 341
b) For the year 2007: 544
c) For the year 2008: 584

1.A.1.b Number/percentage of these requests that are generated by type of requesting authority: 1. police, 2. judicial, and 3. other authorities (please specify as relevant) [Quantitative Reply]

Requesting authorities:

a) For the year 2006: 281 requests from the LEAs, 10 requests from the Public Prosecutor and 50 requests from the Investigating Judge.
b) For the year 2007: 451 requests from the LEAs, 11 requests from the Public Prosecutor and 82 requests from the Investigating Judge.
c) For the year 2008: 516 requests from the LEAs, 5 requests from the Public Prosecutor and 63 requests from the Investigating Judge.

1.A.1.c The time elapsed between the date on which the data were retained and the date on which the competent authority requested the transmission of the data, or if unavailable, the average age of the data that are requested, ? The answer to this question may already have been provided in the context of the statistics of Article 10 DRD. [Quantitative Reply]

The time between the date when the data where generated and the date on which the judicial authority issued the order to the Communications Provider varies from one (1) day to three and a half (3,5) years.

1.A.1.e.2 What is the average age of the data that has been requested for the different types of crime mentioned under 1.A.1.e.1 ? [Quantitative Reply]

Please see 1.A.1.c.

1.A.1.j.2 How much does the use of retained data cost in terms of deployment of Human Resources and acquisition & maintenance of dedicated equipment ? What are the typical cost drivers? [Quantitative Reply]

Due to the non implementation of the DRD we are not yet able to answer.
1.A.2. a.3 to 1.A.2.b.3. Please see 1.A.1.j.2.

1.A.3.a.7 Centralised storage of data by Service providers

Does your country have problems (e.g. time to obtain an answer, quality of the reply) to obtain retained data that are stored by service providers outside of your country. Please provide details of problems you may have experienced and means deployed to redress these problems. [can entail Quantitative elements]

Service Providers store data within the Hellenic territory.

1.B.1.e Which training or skill-development scheme, if any, does your Member State provide for law enforcement authorities to train them in attributing (linking) end-user devices (e.g. mobile phones) to data that are held by communication providers to identify the end-users?

1.B.1.e. Please see 1.A.1.j.2.
GREECE

1 QUESTIONS TO MEMBER STATES AND AND NON-EU EEA STATES

1.A Qualitative and quantitative aspects of the application of Directive 2006/24/EC, taking into account further developments in electronic communications technology and the statistics provided pursuant to Article 10,

1.A.1 Law enforcement issues

1.A.1.a Total number of requests that are issued by year to obtain data retained under the DRD [Quantitative Reply]

We shall reserve replying to you until 15 December 2009 (Quantitative)

1.A.1.b Number/percentage of these requests that are generated by type of requesting authority: 1. police, 2. judicial, and 3. other authorities (please specify as relevant) [Quantitative Reply]

We shall reserve replying to you until 15 December 2009 (Quantitative)

1.A.1.c The time elapsed between the date on which the data were retained and the date on which the competent authority requested the transmission of the data, or if unavailable, the average age of the data that are requested, ? The answer to this question may already have been provided in the context of the statistics of Article 10 DRD. [Quantitative Reply]

We shall reserve replying to you until 15 December 2009 (Quantitative)

1.A.1.d Which communication channels are used to exchange information between law enforcement authorities and service providers (e-mail, fax, secure network, or other channels)? If certain channels are required to be used, please provide information about the channels to be used

The requested information are handed over either by secure mail and secure fax, or semi electronically (CD’s).

1.A.1.e Type of crimes

1.A.1.e.1 For what types of crime does the national law authorise the acquisition and use of retained data? Please provide a list of these crimes

Act 2225/94 (article 4 par. 1) provides access to communication data for the (pre trial) criminal investigation of offences which are exhaustively listed in the statutes of this paragraph (no 1), mainly felonies (punishable mainly by custodial penalties, mainly by a term of 5 years to 20 or by life imprisonment):

a) Penal Code: high treason, attempt to murder the Prime Minister etc. political persons, torture and violations of human dignity, treason against the state (actions against State security, rendering military services to enemy services, revealing state secrets, espionage, forgery or concealing or destruction of documents against State interests), offences relating to the free exercise of civil rights (violence
against Parliament, members of Parliament or members of Government to avoid or to be obliged to action, bribery), offences against public order (criminal organization—see also article 253A Criminal Procedure Code for criminal organization and terrorism), offences relating to currency (counterfeiting and setting into circulation coins and banknotes), offences relating to civil servants (bribery of servants in public or municipal utility companies, judges), offences relating to common danger (arson, explosions, disabling safety devices in factories or mines), offences against security in transportation (aviation, railway and water transportation), offences against human life (homicide), offences against personal freedom (kidnapping), offences against sexual freedom and relating to the economic exploitation of minors and child pornography, offences against property (theft, robbery), offences against property rights (blackmail). Furthermore, lawful interception may be ordered in case of the offence of planning to commit counterfeiting of banknotes or coins, offences relating to antiquities, child pornography and sexual abuse of minors.


Access to communication data is also allowed under specific requirements and procedure (Act 2225/94 art. 3) for national security reasons.

1. A.1.e.2 What is the average age of the data that has been requested for the different types of crime mentioned under 1.A.1.e.1? [Quantitative Reply]

We shall reserve replying to you until 15 December 2009 (Quantitative)

1. A.1.e.3 Does the national law allow for or prohibit acquisition of data from communications providers of data subservient of the Directive and/or related instruments for purposes other than the investigation, detection and prosecution of serious crime (e.g. copy right infringements). If so, please provide details about the alternative purpose(s) or laws prohibiting such acquisition.

Access to communication data is allowed only for national security reasons and investigation and prosecution of particularly serious crimes, which are exhaustively listed in the law, meaning that it is prohibited access to communication data for any crime which is not contained in the list.
1.A.1.e.4 Assessment of the data to be retained

1.A.1.e.5 Does the national law transposing the Data Retention Directive or a related instrument, require the retention of other categories of data in addition to the data contained in Article 5 of the Directive? If so, please provide details about the additional data as well as the instrument in which this obligation is enshrined.

According to the Hellenic legal framework, there is no adoption of any legislative measure for the **obligatory** retention of data for national security reasons, defence, public security and the prevention, investigation, detection and prosecution of criminal offences, because of the non implementation of DRD.

1.A.1.e.6 Adequacy and law enforcement relevance of the data retained under Article 5 of the Data Retention Directive

The data that the service providers must retain under article 5 are relevant and sufficient from a law enforcement perspective at present. In the future, due to technological progress in the area of electronic communication, it shall be necessary to add data which may provide useful information.

1.A.1.f Details of the requests that are issued

1.A.1.f.1 The kind of information that service providers are requested to retrieve: Please provide information about typical search parameters (information selection criteria) contained in requests for the acquisition of retained data, e.g. listing of the communications made from or to a given phone number, or on certain date, or at a certain hour, or listing of all calls made from a certain location, or of all numbers used by an identified user.

Typical search parameters are: In the telephony area: list of incoming and outgoing calls (numbers) of a given phone number (target of the investigation), date, time and duration of incoming and outgoing calls, name and address of calling and called party, IMEI, IMSI, Cell ID. In the internet area: name and address of the subscriber or registered user to whom an IP address was allocated in a specific date and time.

1.A.1.f.2 Did your country standardise or seeking to standardise the format for the acquisition and disclosure of communications data between public authorities and communications service providers (for instance in service level agreements, or by making reference to relevant ETSI standards)? If so, please provide information about the standard (form or format) for requests, the message format, the technical modalities and/or interface.

Services providers and LEAs apply the ETSI standards for Lawful Interception (content of communication). The competent independent administrative authority
(A.D.A.E.) is in favor of the ETSI standards also for communication data, but there is no provision for standardization, because of the non implementation of the DRD.

1.A.1.g Details of the replies to the requests mentioned under 1.A.1.g

1.A.1.h Does the national law governing the acquisition of communications data enable the public authority to specify the time period within which data must be disclosed, as referred to in the Directive as “without undue delay”. If so:

Presidential Decree 47/05 (article 6) provides for the obligation of the Service Provider to install, the required for the lawful interception, hardware and software, which is obliged to activate for the execution of the judicial order, within three (3) hours from the receipt of the judicial order. In case data cannot be immediately disclosed, P.D. 37/05 provides the storage of data and the disclosure within 7 days.

1.A.1.h.1 Please provide examples of time frames enforceable within the context of national legislation or by service level agreements between competent authorities and communication providers.

There is no provision for service level agreements between competent authorities and communication providers.

1.A.1.h.2 What measures do competent authorities avail of to ensure the respect of the time period within which they request the reply to be given?

Presidential Decree 47/05 (article 8) provides the obligation of Service Provider to immediately respond to the judicial order for the disclosure of the requested data. In case of non compliance to this obligation, the competent independent administrative authority may issue Recommendation to the Provider, or impose an administrative sanction (e.g. fine). However, article 5 par. 11 Act 2225/94 provides that penal sanctions shall be imposed for the employees of the SP who shall not comply with the judicial order by means of not providing to the competent authority technical assistance or information ordered (by the judicial council) to be provided.

1.A.1.h.3 Where relevant, do competent authorities distinguish between time periods within which they require the disclosure of data by communication providers and the type of request or type of data they need? If so, please provide examples of such differentiation.

No, there is no provision for such a distinguish.

1.A.1.i Reimbursement of costs

1.A.1.i.1 Does your country reimburse CAPEX\(^4\) and/or OPEX\(^2\) incurred by service providers? If so, please provide information about the type of costs that are reimbursed, as well as about the modalities and amount or ratio of reimbursement.

As a rule, there is no reimbursement of CAPEX or OPEX. In particular cases, such as leased recording lines (the link between the Service Provider and the LEA for the
lawful interception procedure, only for the content of communication) there is a fee for the leasing of the line.

1.A.1.i.2 Does your country make the reimbursement of costs conditional on the respect of certain conditions, such as, for instance, guaranteeing a certain quality of service (request profiles, amount of requests to be handled, speed of retrieval)? If so, could you please provide information about the conditions that service providers have to meet and the link between reimbursement scheme.

No, there is no such provision.

1.A.1.j Effectiveness - What is the success rate of the use of retained data

1.A.1.j.1 Did the use of retained data assist in crimes being detected and/or prosecuted within the courts that otherwise would have failed? If so, please provide examples [can entail Quantitative elements]

Yes, the use of communication data assist in crimes being investigated and prosecuted within the courts that otherwise would have failed.

1.A.1.j.2 How much does the use of retained data cost in terms of deployment of Human Resources and acquisition & maintenance of dedicated equipment? What are the typical cost drivers? [Quantitative Reply]

We shall reserve replying to you until 15 December 2009 (Quantitative).

1.A.1.j.3 How can cost-effectiveness of the acquisition and use of retained data be increased? [Entails quantitative elements]

We shall reserve replying to you until 15 December 2009 (Quantitative).

1.A.2 National and transnational requests and answers

1.A.2.a.3 how many (a) incoming and how many (b) outgoing transnational requests are processed by your country on an annual basis. When possible, please differentiate between judicial co-operation and non-judicial cooperation [Quantitative Reply]

1.A.2.a Within this questionnaire, a "transnational request" means a cross-border request for the acquisition of communications data between EU Member States and non-EU EEA States as appropriate where:

1.A.2.a.1 law enforcement authorities from another country requests you to provide data retained by service providers within your country (the "incoming requests") and

1.A.2.a.2 requests initiated by your competent authorities for data held within another country's jurisdiction (the "outgoing requests").

1.A.2.a.3 how many (a) incoming and how many (b) outgoing transnational requests are processed by your country on an annual basis. When possible, please differentiate between judicial co-operation and non-judicial cooperation [Quantitative Reply]

We shall reserve replying to you until 15 December 2009 (Quantitative).
We shall reserve replying to you until 15 December 2009 (Quantitative).

1.A.2.b  What is the average time to:

1.A.2.b.1 receive an answer to an outgoing request, between the moment of issuing the request and the reception of the answer (see also A.A.2.f)? What are the elements (for instance: type of procedure) that determine the length of the procedure? [Quantitative elements]

We shall reserve replying to you until 15 December 2009 (Quantitative)

1.A.2.b.2 provide an answer to an incoming request, between the moment of reception of the request and the sending of the answer? What are the elements (for instance: type of procedure) that determine the length of the procedure? [Quantitative elements]

We shall reserve replying to you until 15 December 2009 (Quantitative).

1.A.2.b.3 Which strategies could be deployed to reduce the time it takes to answer an incoming request?

We shall reserve replying to you until 15 December 2009 because it is in accordance with the previous quantitative questions.

Ju

1.A.2.c  Which authority takes the decision in your country to issue a transnational request? Are all law enforcement authorities entitled to make or prompt to make a transnational request?

Transnational requests are issued by judicial authorities according to the European Convention on Mutual Legal Assistance in criminal matters. Schengen Treaty is also applied and especially article 53 which provides with the potentiality for the judicial authority to issue a request.

In any other case, where the Schengen Treaty is not applied, article 457 – 461 Code of Criminal Procedure is applied, where the competence lies with the judicial authority. There is also use of www.ejn-crimjust.europa.eu (ATLAS system).

1.A.2.d Does your country have a central point that issues outgoing requests or receives incoming requests? If so, please provide details about these central points.

In particular cases, the central point may be the Ministry of Justice.

1.A.2.e  Costs

1.A.2.e.1 If your country reimburses OPEX (see 1.A.1.k) do you reimburse national service providers in the same way for replying to transnational requests? Do you or do you plan to ask other Member States to share the costs?
There is no OPEX reimbursement.

1.A.2.f  Language

1.A.2.f.1  Does your country impose linguistic conditions to incoming requests (e.g. translation in a national or vehicular language? If so, please provide details about those conditions.

Under the regime of Schengen Treaty applies in Greek language.

In any other case incoming requests are not subject to linguistic conditions.

1.A.2.f.2  What means does your country deploy to comply with linguistic conditions imposed by other countries to outgoing requests? Do you have a central facility to provide linguistic support?

Linguistic support is given, when needed, by the Ministry of Foreign Affairs (Translation Service).

1.A.2.g  Data security

Act 3674/08 on ensuring the Security of privacy and secrecy in telecommunications sector, provides that service providers are obliged to take the appropriate technical and organizational measures to safeguard security of its services, its premises, equipments, hardware, software and any kind of systems for publicly available telecommunications services. Competent independent administrative authority (A.D.A.E.) shall issue Regulations for ensuring the security of the communication and the Providers are obliged to apply these Regulations. The provider is obliged to have a special security policy, which is approved by A.D.A.E.

Act 3471/06 (implementation of Directive 58/02/EC) provides that the Provider is obliged to take the appropriate technical and organizational measures to safeguard security of its services and the security of the publicly available network. A.D.A.E. conducts inspections and audits at the installations, equipments, archives, databases and documents of the Hellenic National Intelligence Service (NIS) and Service Providers in order to ensure the application of the legal framework for the protection of confidentiality of communications, for the procedure of lawful interception and for the security of the services, the network, the hardware, the software and data.

Administrative, civil and penal sanctions shall be imposed in case of violation of the legal framework for the security of data.
1.A.3 Telecommunications authorities

1.A.3.a Allocation of tasks

1.A.3.a.1 Which national authorities are charged with tasks resulting from the Directive (for instance, as appropriate, following up with relevant service providers about applicable law, specifying content of data to be retained e.g. in CDRs, providing for a certain standardisation e.g. on the basis of ETSI standards, managing reimbursement schemes, assessing the economic impact of the implementation and application of the Directive)? Which tasks are assigned to which authority?

The DRD has not yet been implemented, so there is not a legal provision about which authority shall be designated to be responsible for monitoring the application of the Directive (art. 9 par. 1 DRD).

Currently, “Hellenic Authority for Communication Security and Privacy” (A.D.A.E. – www.adae.gr) is the administrative independent authority which is responsible for ensuring the confidentiality/secrecy of letters and all other forms of free correspondence or communication, for ensuring the procedure (especially between the CSP and the LEA) of lawful interception and access to communication data, for ensuring the security of communication for publicly available electronic communication services.

A.D.A.E. has been established by Act 3115/03 due to a Constitutional provision.

Article 19 par. 1 states: “Secrecy of letters and all other forms/means of free correspondence or communication shall be absolutely inviolable. The guaranties, under which the judicial authority shall not be bound by this secrecy for reasons of national security or for the purpose of investigating particularly serious crimes, shall be specified by law”.

Article 19 par. 2 states: “Issues relating to the constitution, the operation and the functions of the independent authority ensuring the secrecy of paragraph 1 shall be specified by law”, which is Act 3115.03.

A.D.A.E. has issued several Regulations for the Security of communication and the technical procedure for lawful interception. ADAE’s main responsibilities, according to Act 3115/03 (articles 6 and 11) are:

a) Inquiring and conducting inspections and audits at the installations, equipments, archives, databases and documents of the Hellenic National Intelligence Service (NIS)
and Communication Service Providers (CSP) in order to ensure the application of the legal framework for the protection of confidentiality of communications, for the lawful interception and for the security of the services, the network, the hardware, the software of the CSP.

b) Gathering of information from NIS and CSPs, as well as from the supervising competent Ministers.

c) Summoning of administrations’ persons, legal representatives and employees of the CSPs, as well as of every other individual having useful information.

d) Confiscating any means used for violating the confidentiality/secrecy of communications and destructing data which has been illegally accessed and gathered.

e) Investigating and examining complaints regarding the protection of the applicants’ rights during the procedure of lawful interception.

f) Issuing instructions, recommendations, opinions and regulations for ensuring confidentiality/secrecy of communication, security of communication and the procedure of lawful interception.


g) Imposing administrative sanctions (e.g. fines) on the CSP in case of violations of the legal framework for the protection of confidentiality/secrecy of communications, for the security of communications and for the lawful interception procedure.

According to Act 3674/08 (article 7) A.D.A.E. is the competent Authority for receiving from Communication Providers every 4 months a Report containing a list of all the judicial orders issued for lawful interception and access to communication data. In the same list, the requesting authorities are mentioned.

Furthermore, each judicial order accepting the request for the lawful interception shall be served to A.D.A.E. (for information) and to the Communication Service Provider (for execution), according to Act 2225/94 (art. 5 par. 4). Consequently, A.D.A.E. is the Authority which is obligatory informed for any judicial order issued in the Hellenic territory and each year issues an Report, containing among others, statistics on the judicial orders.

Despite the fact that Hellenic Data Protection Authority-H.D.P.A. (www.dpa.gr) is responsible for any kind of personal data, A.D.A.E. is also responsible for any issue relating to communications, consequently the communications data. It is important to note that judicial orders issued for access to communication data shall be served only to A.D.A.E. and not to H.D.P.A.
1.A.3.a.2  When did/will the respective authorities start to be operational for these tasks?

The DRD has not yet been implemented. However, A.D.A.E. is operational for the tasks of the current legal framework.

1.A.3.a.3  For each authority: Did/does the authority need to acquire additional expertise in order to perform its tasks under the Directive? Which? How was this implemented (e.g. new staff, reorganisation, special training) or how will it be implemented?

There is no need for A.D.A.E. to acquire additional expertise in order to perform tasks under the DRD, in case it shall be designated as the competent authority, because of the experience from its participation to ETSI Working Group for lawful interception and data retention issues. Furthermore, A.D.A.E. has a large experience due to the audits conducted to Service Providers.

1.A.3.a.4  Does any authority mentioned under this section collect data about the economic effects of measures required under the Directive, including the impact of replying to court orders to provide retained data issued by Civil Courts on the request of copy right owners in cases brought by them against illicit downloading and file sharing of copy right protected material. If the answer to this question is affirmative, please provide details about the authority as well as about the data that are collected? [May entail Quantitative elements]

Offences related to copyright violation and illicit downloading and file sharing of copy right protected material, are not part of the list of article 4 Act 2225/94, under which is allowed access to communication data, after a judicial order.

1.A.3.a.5  Does any authority mentioned under this section engage in cross-border co-operation relating to the Directive? If so, please provide details about 1. those authorities 2. the type of action or activity that these authorities undertake in this context. [May entail Quantitative elements]

It is not clear what kind of cross–border cooperation relating to the Directive, is mentioned. We shall reserve replying to you.

1.A.3.a.6  Do the authorities mentioned under this section gather data concerning the impact of the required measures on competition e.g. on market entry for new operators, on advantages for bigger companies? Please provide details about the kind of data that are being collected! [May entail Quantitative elements]

A.D.A.E. and H.D.P.A. do not collect that kind of data.

1.A.3.a.7  Centralised storage of data by Service providers

Does your country have problems (e.g. time to obtain an answer, quality of the reply) to obtain retained data that are stored by service providers outside of your country. Please provide details of problems you may have experienced and means deployed to redress these problems. [May entail Quantitative elements]

We shall reserve replying to you.
1.B Evaluation of the effectiveness of existing (non-)legislative measures or technical solutions to ensure traceability of users of communications services, in particular mobile phone lines, opened with prepaid SIM cards (cfr Council Conclusions in Annex)

1.B.1 Law enforcement issues

1.B.1.a Which means (technical, operational) or measures (procedural, law-based) does your country deploy to increase the traceability of users of communication services so as to assist law enforcement authorities in the attribution of end-user devices to the person using them? Among the measures mentioned are those that take account of data that are presently held by communication providers, such as customer service notes, payment history, insurance agreements, IMEI history, but also supermarket loyalty cards associated to the top-up history, use of e-top-up linked to debit or credit cards, information held by credit reference agencies and mobile device given as contact point, forensic examination of mobile devices? Please provide a description of these measures.

The traceability of mobile phone users, in particular those using prepaid SIM cards, and the matter of anonymity has been dealt with by the new Act 3783/07-8-09, which impose the obligations on the SP and the users to make identifiable the persons, the services and the mobile equipments for national security reasons and investigation-prosecution of serious crimes (art.1). All users, either subscribers or not, shall be obliged to register with the SP: name, surname, place and time of birth, copy of ID card or Passport or Green card (foreigners permission of staying) and TAX identification number etc. If the user is a legal entity, the same obligation shall exist and it shall be needed to register the name of the company, the registered offices of company, name and surname of the legal representative and number for TAX Authority. There shall be also an obligation for the SP to register the telephone number, IMSI, IMEI, date and time of the first activation of the service, CELL ID, SIM card number. For the new clients (after issuing of the Act), the SP shall be obliged to collect the above mentioned data, which shall be retained in its archive, as a requirement of activating the service. The SP shall activate the service, only upon the condition of declaration of the required data (art 2-3).

The user shall be obliged to register the data and in case he/she sells or gives the SIM, he/she shall inform the SP in writing, otherwise he/she shall be legally considered as the real subscriber, even if he/she shall not be (art. 4 par.2). In case of loss or theft of the mobile phone or SIM card the subscriber shall be obliged to inform the SP, which shall be obliged to interrupt the service. If not, administrative sanctions shall be imposed to the Provider (art. 4 par. 2).
The data shall be retained for a period of one (1) year starting from the end of the connection and then same shall be destroyed (art. 5 par. 1).

1.B.1.b What is the scope of these means or measures in terms of contribution to increasing the traceability of users? Please provide details about the legal justification or administrative motivation and as well as about the scope of these instruments, i.e. whether they are aiming to assist the prevention of crime, or its detection, investigation or prosecution. Which crimes are specifically addressed by the means and measures that your country deploys.

This provision completes the Hellenic legal framework for lawful interception and access to communication data. Anonymous users of pre paid cards may commit serious crimes or put in danger the national security. These measures ensure traceability of anonymous users. Police may access the communication data under the conditions and requirements of Act 2225/94 only for national security reasons and for investigation-prosecution of particularly serious crimes, as above mentioned (please see reply to 1.A.1.c.1.).

1.B.1.c Efficiency

1.B.1.c.1 Are the measures imposed by your country efficient in terms of achieving the aim for which they have been put in place? Please provide details about results obtained as a result of the deployment of the relevant means or measures [may entail Quantitative elements].

According to the Act, the procedure of making identifiable users and mobile equipments shall be completed by the 30 July 2010. Until then, Service Providers shall be obliged to inform the pre – paid cards users, which had anonymous telephone connections prior to this Act, that all pre-paid anonymous services shall be disconnected by 30 July 2010, unless the users declare their identity and submit all the requested documents. Consequently, we are not currently able to make comments on the efficiency of the measures before the completion of the procedure.

1.B.1.c.2 Did your country assess the effectiveness of the measures If so, please provide details of this assessment.

There are no details of any assessment of the effectiveness due to non completion of the procedure (see 1.B.1.c.1.).

1.B.1.c.3 What is the added efficiency of the measures deployed by your Member State in terms of improvement of your capabilities to detect, investigate or prosecute of terrorism and other serious forms of crime that go beyond the results obtained with the data obtained under Article 3(1)(e)(2) of the Directive and in particular its paragraph (vi)? [can entail Quantitative elements]
According to the legal framework, before the said Act, there was no obligation to retain the said communication data. Under the current legal framework, a series of data shall be registered and retained.

1.B.1.c.4 What are the costs or these measures for the private sector? 

There is no cost reimbursement for collecting and retaining the data from the service provider.

1.B.1.d Should measures be taken at European level to increase the traceability of users of communication devices? If so, which measures should be taken, at European level? How would these measures improve the efficiency of the means and measures that you deploy at national level?

We believe that answering the above question is feasible only after evaluating the effectiveness of the relevant provisions on national level. Consequently we are not currently able to make comments.

1.B.1.e Which training or skill-development scheme, if any, does your Member State provide for law enforcement authorities to train them in attributing (linking) end-user devices (e.g. mobile phones) to data that are held by communication providers to identify the end-users?

We shall reserve replying to you.

1.B.2 Telecommunications authorities

1.B.2.a Which impacts on the market do the means or measures mentioned in section 1.B.1 have?

There is not currently knowledge on the impacts due to non completion of the procedure (please see 1.B.1.c.1.).

1.B.2.b Does the authority mentioned in 1.A.3.a. monitor and enforce national measures on providers or other stakeholders?

National Regulatory Commission of Telecommunications and Postal Services (E.E.T.T.) supervise the procedure of the said Act (see 1.B.1.a.) and shall be responsible for monitoring the application of the law.

1.B.2.b.1 Did the authority mentioned in the previous question investigate any cases of non-compliance with national means or measures? Please provide details, if relevent.

There is not currently knowledge due to non completion of the procedure (please see 1.B.1.c.1.).

1.B.2.b.2 If the national law provides for measures to ensure the identification of users of prepaid SIM cards, what treatment is given to the cards acquired before the entry into force of the law? Are these cards cancelled after a certain period in use?
The SIM cards acquired before the entry into force of the law, continue to be used, until the 30 July 2010. Within this time period (from 07/8/09 until 30/7/10) the users shall register to the service provider the requested data. After 30 July 2010 the SIM cards shall be cancelled.

3 **QUESTIONS ADDRESSED TO NATIONAL SUPERVISORY AUTHORITIES AND THE EUROPEAN DATA PROTECTION SUPERVISOR (EDPS)**

The replies of the Hellenic Data Protection Authority are:

**“Hellenic Data Protection Authority (HDPA)”**

3.A Assessment of the application of Directive 2006/24/EC, taking into account further developments in electronic communications technology and the statistics provided pursuant to Article 10\(^{\text{a}}\).Please provide information on the distribution of competences of supervisory authorities according to Directives 95/46/EC, 2002/58/EC and 2006/24/EC.

The Directive 2006/24/EC has not yet been transposed into the Greek legal system.


HDPA is responsible for the supervision of Law 2472/1997. It is also supervising Law 3471/2006, except from the cases where specific responsibilities have been assigned to other national supervisory authorities, i.e. ADAE – National Authority for the Secrecy of Communications- is responsible for the case of elimination of presentation of calling line identification with regard to malicious, nuisance and emergency calls (art. 8 par. 7 Law 3471/2006) EETT – National Commission for Telecommunications and Post- is only responsible to issue an opinion in the matter of whether it is technical possible to provide specific services anonymously or using pseudonyms (art. 5 par. 7 Law 3471/2006).

3.A.1 Do authorities have investigative powers vis-à-vis providers? Which cases of complaints, if any, that have led to supervisory or investigative activities? Please provide for an overview of these activities and the outcome of proceedings.

3.A.2 Do authorities have investigative powers vis-à-vis public authorities? Which cases of complaints, if any, that have led to supervisory or investigative activities? Please provide for an overview of these activities and the outcome of proceedings.

HDPA has investigative powers vis–a-vis providers and public authorities according to articles 19 of Law 2472/1997 and 13 of Law 3471/2006. So far, the authority has not received any complaints concerning the use of retained data within criminal investigations and, thus, no relevant supervisory or investigative activities have been performed.

It is worth mentioning a recent Opinion of the Attorney General of the Areopag (i.e. the Hellenic Supreme Court of civil and penal law matters), according to which the law enforcement authorities may have access to electronic communications’ traffic
data, when a crime is committed through the Internet in general, but also more specifically through blogs (defamatory or abusive comments/posts) from anonymous users. The opinion states that a communication taking place through a blog is by definition public and, since the content of it has been made public, the police authorities are therefore allowed to request the ISPs to identify the anonymous users through the traffic data, i.e. IP-addresses.

(Please note that for certain offences that are considered as serious crimes, it is lawful to intercept the confidentiality of communications upon court order, such as for crimes of child pornography via the Internet. However, violations of copyright have not been added to this list).

The ISPs recently submitted a query to HDPA as to whether it is legal to supply this data to the law enforcement authorities. HDPA has not yet issued an opinion on the matter.

3. A. 3 Do authorities have the power to audit the compliance of providers and have there been any audits? If so, please provide details about such audits and the outcome of proceedings. [can entail Quantitative elements]

HDPA has the power to audit compliance of providers according to articles 19 of Law 2472/1997 and 13 of Law 3471/2006. With regard to data retention, HDPA participates in the 2nd joint supervisory activity of the Article 29 Working Party concerning the application of Directives 2002/58/EC and 2006/24/EC. In the context of this action, providers have to fill a data retention specific questionnaire. The HDPA is currently conducting on site audits which focus on the providers’ obligations according to Directive 2002/58/EC. The final report of the audits will be submitted to the article 29 working party in December 2009.

3. A. 4 Which problems have supervisory authorities identified with the practical implementation of the Directive? (legal, practical, other; please provide details) [can entail Quantitative elements]

N/A.

3. A. 5 What experience do authorities have with the supervision of data that service providers have stored centrally, i.e. either within their jurisdiction or beyond? If so, please provide details about the challenges met in that context, also with regard to data stored outside of the EU/EEA. Please specify in particular the data protection issues that have been addressed that context and the approach that has been followed to settle the contentious issues. [can entail Quantitative elements]

Please, see answer to question 3. A. 3.

3. A. 6 Please provide details about case law (jurisprudence), if any, with regard to the implementation or use of the Data Retention Directive or concerning the use of retained data within criminal investigations?

N/A.
In July 2009 a new Law was introduced in the Greek legal system about the identification of owners and users of mobile phone equipment and services (Law 3783/2009), which aims at ensuring traceability of users of communication services with pre-paid SIM cards.

More specifically, providers have to collect personal data of identification from current and new users of pre-paid mobile phones. For the current users, this has to be completed by 30/6/2010. If a subscriber fails to submit to the provider their identification data by 30/7/2010, then the provider must proceed with the disconnection of the service to this subscriber/user.

Providers have the obligation to retain this data for up to a year after the last use of the number/service, and there should not be a cost involved for the users.

Identification data that needs to be collected for the subscriber includes name, name of father, place and date of birth, photocopy of national ID card or passport and the national tax payer registration number.

But, data needs also to be collected for the identification of the mobile device, such as the IMSI (International Mobile Subscriber Identity) and IMEI (International Mobile Equipment Identity) number, as well as the time and place (cell-id of the closest antenna mast). Every SIM (subscriber identity module) card sold has to be paired to an identified subscriber. The subscribers are obliged to notify the provider in writing of any changes to the pre-paid mobile phone, such as loss, theft, or even allowing someone else to use (in cases of letting someone else use the phone, both users have to notify the provider in writing).
Access to this data stored by the operator will be available only to the law enforcement authorities according to the provisions for the lawful interception, i.e. only for (serious) crimes as listed in the law.

Currently, according to recent estimates, there are 13.5 million of anonymous pre-paid mobile phones in Greece, of which 9 million are active connections. Only 5 million are registered (i.e. the user/subscriber is identified).

HDPA has not formally issued an opinion on the provision of the aforementioned Law. Since the Law is quite recent there has not been yet any evaluation of its effectiveness and related data protection issues”.

As fas as A.D.A.E. is concerned:

3.A.1. A.D.A.E. as already mentioned (please see 1.A.3.a.1.) has investigative powers vis a vis providers, under administrative (and not criminal) law. A.D.A.E. has the responsibility to conduct audits, inspections, searches etc. investigative actions in order to ensure the application of the legal framework for the protection of confidentiality of communications, for the application of its Regulations (for security matters, for malicious or nuisance calls and for Emergency Calls such as E112 lines [please see art. 10 E- Privacy Directive]) for the lawful interception and for the security of the services, the network, the hardware, the software of the Service Provider.

3.A.2. A.D.A.E. as already mentioned (please see 1.A.3.a.1.) has investigative powers vis a vis public authorities, especially the National Intelligence Service (N.I.S.) and any public Service Provider.

3.A.3. A.D.A.E., as already mentioned (please see 1.A.3.a.1.), has the power to audit the compliance of providers to the current legal framework for the security and confidentiality of communication, for the procedure of lawful interception etc. In specific cases A.D.A.E. has imposed to Providers administrative sanctions (fines) for violating the current legal framework.

3.A.4. The DRD has not yet been implemented.

3.A.5. The DRD has not yet been implemented.
3.A.6. The DRD has not yet been implemented.
3.B. There are no details of any assessment of the effectiveness due to non completion of the procedure (see 1.B.1.c.1.).

4. **QUESTIONS TO THE PRIVATE SECTOR.**
   
   We shall reserve replying to you.