CONTRIBUTION FROM BULGARIA
17/11/2009

QUESTIONNAIRE
WITH A VIEW TO TAKE 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

1. QUESTIONS TO MEMBER STATES 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]

ANSWER: No information available.

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]

ANSWER: No information available.

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]

ANSWER: No information available.

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

ANSWER: Personally delivered to the claimant on paper or by a
specialized express service.

¹ As to 9 November 2009 the relevant Bulgarian legislation is being amended in order to be in full compliance
with the Directive 2006/24/EC
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

ANSWER: For serious crimes. According to Art. 93 of the Penal Code "Serious crime" is a crime for which the law stipulates a punishment of imprisonment of more than five years, life imprisonment or life imprisonment without an option.

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 I.A.1.e.1? [Quantitative Reply]

ANSWER: No information available.

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. copyright infringements). If so, please provide details about the alternative purpose(s) or laws prohibiting such acquisition.

ANSWER: The legislation of the Republic of Bulgaria prohibits data retention and the use of the retained data for purposes other than the investigation, detection and prosecution of serious crimes.

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.

ANSWER: National law does not require the retention of categories of data other than the data contained in Article 5 of the Directive.

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

Please indicate whether the data the service providers must retain under Article 5 of the Directive are relevant and sufficient from a law enforcement perspective, and mention which data either should be removed
from the list of Article 5 where redundant or be added where relevant data is not yet retained.

Member States are invited to motivate their answer and provide examples of situations that demonstrate the redundancy or the law enforcement requirements.

ANSWER: The data categories that must be retained under Article 5 of the Directive completely meet those requirements of the Law enforcement authorities of the Republic of Bulgaria.

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.

ANSWER: According to the acting legislation of the Republic of Bulgaria the service providers must retain and retrieve the following information:

- Listing of all calls made by a definite subscriber or user – incoming and outgoing calls within a concrete time interval.
- Listing of all calls made from a certain location within a concrete time interval,
- Identification data of the owner or user of the communication device-IMEI, IMSI, MSISDN.

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.

ANSWER: No information available.
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:

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.

ANSWER: There is no such existing national authority.

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?

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.

ANSWER: There are no different time intervals throughout which the retained data is stored according to the competence of the law enforcement authorities.

1.A.1.i Reimbursement of costs

1.A.1.i.1 Does your country reimburse CAPEX and/or OPEX 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

ANSWER: Under the acting legislation of the Republic of Bulgaria the costs are not reimbursed.

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 schemes.

ANSWER: The costs are not reimbursed.
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]

ANSWER: The data is of significant importance in the process of revealing crimes. No information is available for any concrete cases.

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]

ANSWER: No information available.

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

ANSWER: No information available.

1.A.2. National and transnational requests and answers

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”).

Having regard to the total number of requests mentioned under section 1.A.1.a:

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 Replies]

ANSWER: No information available.

1.A.2.a.4 what is the ratio between national and transnational requests (total number of transnational requests)? [Quantitative Reply]
ANSWER: No information available.

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]

ANSWER: No information available.

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]

ANSWER: No information available.

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

ANSWER: No information available.

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?

ANSWER: All law enforcement authorities are empowered to issue or require a transnational request in accordance with its competence.

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.

ANSWER: There is no such central unit established.

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?

ANSWER: The Republic of Bulgaria does not reimburse the costs.
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.

ANSWER: No linguistic conditions are required to incoming requests.

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?

ANSWER: Translation is effected, but there is no central facility to provide linguistic support.

1.A.2.g Data security

Which measures (rules, procedures, audit provisions) are enforced to protect data against misuse?

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?

ANSWER: There are no specialized national authorities charged with the task resulting from the Directive.

1.A.3.a.2 When did/will the respective authorities start to be operational for these tasks?

ANSWER: There are no specialized national authorities charged with the task resulting from the Directive.

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?
ANSWER: There is no need for additional expertise in order to perform the tasks resulting from the Directive.

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 copyright owners in cases brought by them against illicit downloading and file sharing of copyright 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]

ANSWER: There is no such authority.

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]

ANSWER: There is no such authority.

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! [Last par may entail Quantitative elements]

ANSWER: There is no such authority.

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]

ANSWER: No information available.
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)

ANSWER: Under the acting legislation there will be no anonymous pre-paid SIM-cards allowed beginning from 1st of January 2010.

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.

ANSWER: Under the acting legislation there will be no anonymous pre-paid SIM-cards allowed beginning from 1st of January 2010. After collecting, processing and delivering of those data to the law enforcement authorities we envisage increasing the traceability of users of communication services.

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?

ANSWER: The undertaken measures are aiming to assist revealing all crimes under Art.93 of the Criminal Code.

They are relevant both to prevention of crimes as well as to revealing crimes and documentary evidence of the criminal activities of the executants.

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].

ANSWER: No information available.

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

ANSWER: No such is affected.

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 5(1)(e)(2) of the Directive and in particular its paragraph (vi)? [can entail Quantitative elements]

ANSWER: No information available.

1.B.1.c.4 What are the costs or these measures for the private sector? [can entail Quantitative elements]

ANSWER: No information available.

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?

ANSWER: Exchange of information between the operators and the providers of communication services and the standardization of the data in accordance with the latest ETSI researches.

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?

ANSWER: There are no skill-development or training schemes established.
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?

ANSWER: No information available.

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

ANSWER: No information available.

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 relevant. [can entail Quantitative elements]

ANSWER: No information available.

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?

ANSWER: Under the acting legislation there will be no anonymous pre-paid SIM-cards allowed beginning from 1st of January 2010. In accordance with the Electronic Communication Act, the regulations with respect to the already owned prepaid SIM cards are clearly defined by the regulatory authority, i.e. The Communication Regulation Commission.

These rules are accessible for the public and are executed by the operators.