INTRODUCTION

- Scope of the questionnaire

This questionnaire seeks to gather information about all relevant aspects of the operation of the Data Retention Directive that will allow the Commission to paint a picture of its practical functioning that is as complete as possible. On that basis, the Commission will draft the evaluation report mentioned in Article 14 of the Directive, which is due for 15 September.

Moreover, the Commission intends to use the questionnaire as a guideline for the meetings that it intends to organise with Member States and non-EU EEA States individually between the end of September and the end of November according to a time table to be agreed upon in the meeting of 10 September.

This questionnaire contains two sets of questions for stakeholders that are concerned by the operation of the 2006 Data Retention Directive (DRD).

The first group of questions aims at providing the European Commission with feedback necessary to assist it in the evaluation of the Directive further to its article 14.

Article 14 DRD states:

1. No later than 15 September 2010, the Commission shall submit to the European Parliament and the Council an evaluation of the application of this Directive and its impact on economic operators and consumers, taking into account further developments in electronic communications technology and the statistics provided to the Commission pursuant to Article 10 with a view to determining whether it is necessary to amend the provisions of this Directive, in particular with regard to the list of data in Article 5 and the periods of retention provided for in Article 6. The results of the evaluation shall be made public.

2. To that end, the Commission shall examine all observations communicated to it by the Member States or by the Working Party established under Article 29 of Directive 95/46/EC.

The second set of questions aims at obtaining feedback to carry out the analysis that was requested by the JHA Council at its meeting of 27 and 28 November 2008. In its Conclusions (see annex) the Council asked the Commission to evaluate 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. The Member States
undertook to “supply, at the request of the Commission, all relevant information on legislative and non-legislative measures or technical solutions implemented to identify users of communications media, and their degree of operational effectiveness”. This questionnaire contains the specific requests from the Commission to obtain the relevant information.

The evaluation will therefore consist of two strands, namely, the assessment of
- the degree to which the Data Retention Directive is fit for purpose, i.e. to establish the extent to which the harmonisation of obligations on information service providers (ISPs) is able to ensure that data are available for the purpose of the investigation, detection and prosecution of serious crime, and
- the degree of effectiveness of national measures to trace the identity of users to combat the criminal misuse and anonymous use of electronic communications.

- Stakeholders concerned

The stakeholders that are concerned by these two sets of questions are the following
1. EU Member States and EEA States and in particular a. law enforcement authorities (Ministries of Interior, and of Justice) and b. telecommunication authorities (Ministry of Telecommunication, National Regulatory Authorities)
2. European Parliament and Civil Society
3. National data protection authorities and the European Data Protection Supervisor (EDPS)
4. Private sector (communications service providers, comprising internet service providers, fixed and mobile telecom operators, network and cable operators, etc)

- Preparation of the questionnaire

The questionnaire was prepared by DG JLS and DG INFSO in particular on the basis of input received from the conference "Towards the Evaluation of the Data Retention Directive" of 14 May 2009. It was discussed for the first time by the Subgroup "Evaluation" of the Experts' Group on Data Retention on 9 September 2009 and presented to Member State representatives on 10 September 2009 in a meeting in the Secure Zone of DG JLS in Brussels.

The Subgroup “Evaluation” is composed in the same manner as the Experts’ Group on Data Retention, i.e. by representatives of Member States, Industry, Data Protection and Parliament.

The Commission intends to ask Member States and non-EU EEA States to comment on the questionnaire until 17 September 2009, and to submit a final questionnaire thereafter.

The questionnaire will be the backbone of the evaluation process.

- Content of the questionnaire

The questionnaire consists of two types of questions: qualitative questions that examine the modalities of and conditions under which the Directive operates, and quantitative questions to gauge data volumes, financial, technological and legal impacts, and ratios between different aspects.

The Subgroup “Evaluation” was of the opinion that replying to the qualitative questions would require less time than providing quantitative data.
In the questionnaire indicates all questions that require a quantititative reply as follows: “[Quantitative Reply]”

- **Time table for replying to the questionnaire**

This version of the questionnaire was handed out to Member States during the meeting of 10 September 2009. The Commission requested Member States to give their views on the content and form of the questions until 17 September, in view of issuing a final questionnaire on 21 September.

According to the Subgroup “Evaluation” a period of eight weeks is a reasonable period to formulate answers to the quantitative questions, and a period of twelve weeks reasonable to gather information necessary to answer the quantitative questions.

For that reason, the Commission would like to receive answers to the first type of questions by 15 November 2009, and the second type of questions (quantitative) by 15 December 2009.

**Processing of confidential or classified information**

The replies to the questionnaire will not be made public by the Commission, but only serve the evaluation of the operation of the Commission. Aggregated results that will not expose individual Member States may be disclosed to illustrate certain positions and statements contained in the evaluation report.

Replying to certain questions may require the disclosure of confidential or classified information.

Respondents are requested to indicate in their answer to the questionnaire whether answers will be confidential or classified and to provide these answers separately via the appropriate procedure.

The Commission undertakes that the information that will be identified as such, will be kept in the Secure Zone and will only be accessible to persons that have the appropriate clearance.

This information can provide, however, essential insight in certain aspects of the operation of the Data Retention Directive. Even under disclosure rules contained in Regulation 1049/2001 this information will remain barred.

**Comments about data categories**

The Data Retention Directive covers three types of operational data: 1. Data concerning fixed network telephony; 2. Data concerning mobile telephony and 3. Data concerning Internet access, Internet e-mail and Internet telephony.

The subgroup “Evaluation” of the Experts Group on Data Retention is of the opinion that in case precise quantitative data can not (yet) be provided, it is much easier to provide the ratio between the different categories of data, in particular since the ration between Internet data in comparison to telephony data is changing in favour of the first.

**Definition of “Request”**

The Subgroup “Evaluation” noted that one “request” (cf Article 8 and 10(1) of the Directive and under1.A.1 below) can concern several (many) “data”. The number of requests can therefore be significantly smaller than the number of data that are transmitted. Depending on
the context, the answer should refer to the total number of requests or of data that are provided.

Throughout the first set of questions (on the evaluation of Data Retention Directive) the expression “country” is used to denote the fact that the addressees of the questionnaire are not only the EU Member States, but also non-EU EEA States.

1 QUESTIONS TO MEMBER STATES AND BY 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]

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) [Quantitative Reply]

1.A.1.c What is the average age of the data that are requested? [Quantitative Reply]

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

1.A.1.e Type of crimes

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

The national law, Law 298/2008 provides in art. 1 that the use of retained data is authorised for the purpose of the investigation, detection and prosecution of serious crime. The serious crime is defined in art. 5 paragraph 1, letter f from Law nr. 298/2008 in the following way: The serious crime is the crime provided in art. 2 letter b from Law 39/2003 concerning the prevention and the fight against organized crime, in the Chapter IV from Law 535/2004 concerning prevention and the fight against terrorism and also the crimes against the security of the state provided in Romanian Penal Code, the special part.
These serious crimes are the following:

Crimes provided in Law 39/2003:
- Homicide, second degree murder, first degree murder
- Illegal deprivation of freedom
- Slavery
- Blackmail
- Crimes against the patrimony with serious consequences
- Crimes of non-observance of the regime of arm and ammunition, non-observance of the regime of nuclear materials and other radioactive matters, and of non-observance of the regime of explosives,
- Money or other values forgery
- Unlawful disclosure of economic secrecy, unlawful competition
- The non-observance of the provisions concerning import/export operations, embezzlement of funds, non-observance of the provisions concerning the import of waste materials and residuum and waste materials
- The procurement
- Crimes regarding gambling
- Crimes regarding drugs traffic
- Crimes regarding trafficking in human beings or crimes related with it
- Immigrants traffic
- Money laundry
- Corruption, crimes assimilated to the corruption, or crimes related with corruption
- Smuggling
- Fraudulent Bankruptcy
- cybercrime
- Trafficking in human tissues or organs
- any other crime for which law provides jail penalty, whose special minimum is for the less 5 years.

Art. 2 Law 535/2004 concerning the fight against terrorism:
- act of terrorism: the facts made by terrorist entities which fulfil the following conditions:
  a) they are usually committed through violence and they cause states of disquiet, uncertainty, fear, panic or terror among the population;
  b) they seriously infringe upon both specific and non-specific human factors and material factors;
  c) they are aimed at specific objectives, of political nature, by determining the State authorities or an international organisation to ordain, to renounce or to influence the making of a decision in favour of the terrorist entity.

- If committed in the conditions provided in article 2, the following offences shall be terrorist acts:
  a) offences of homicide, second degree murder and first degree murder, as provided in art.174-176 of the Criminal Code, bodily injury and serious bodily injury, as provided in art.181 and art.182 of the Criminal Code, and illegal deprivation of freedom, as provided in art.189 of the Criminal Code;
b) the offences provided in art.106-109 of the republished Government Ordinance no.29/1997 on the Aerial Code;
c) offences of destruction, provided in art.217 and art.218 of the Criminal Code;
d) offences of non-observance of the regime of arm and ammunition, non-observance of the regime of nuclear materials and other radioactive matters, and of non-observance of the regime of explosives, provided in art.279, art. 279\(^1\) and art. 280 of the Criminal Code;
e) production, acquisition, possession, transportation, supply or transfer to other persons, either directly or indirectly, chemical or biological arms, and research in this field or development of such arms;
f) introducing or spreading into the atmosphere, on the soil, into the subsoil or into water, products, substances, materials, micro organisms or toxins that are likely to jeopardise the health of persons or animals or the environment;
g) threatening with the commission of the acts in a)-f).

(2) Terrorist acts provided in para.(1), shall be punished as follows:
a) for the offences in para.(1) a)-d), the maximum of the punishment of imprisonment provided in the law shall be increased by 5 years, while not exceeding the general maximum of the penalty of imprisonment and the penalty of interdiction of certain rights shall be applied as well;
b) for the offence in para.(1) e)-f), the punishment shall be inprisonment from 15 to 20 years and the interdiction of certain rights, and for the offence in para.(1) g) the punishment shall be imprisonment from 3 to 10 years and the interdiction of certain rights.

(3) For offences of destruction provided in art.217 of the Criminal Code, if they are committed in the conditions in para. (1), the fine shall not be applied.

(4) Attempt shall be punished.

(5) The production or acquisition of means or instruments, and the taking of measures in view of committing the offences in para.(1) shall be considered attempt.

– (1) The following acts shall be assimilated with terrorist acts:
a) acquisition, possession, manufacture, fabrication or supply or, the case being, production of means of destruction, of toxic substances, of pernicious materials, micro organisms or other substances, which are likely to jeopardise the health of people or animals or the environment, for terrorist purposes;
b) recruitment, instruction or training of terrorist entities with the view of using firearms, ammunition, explosives, chemical, biological, bacteriological or nuclear weapons, and in view of facilitating or committing terrorist acts;
c) facilitating the entry/exit, into/of our country, housing or facilitating access to the area of targeted objectives of a person about whom it is known that he supported/committed or is going to support/commit a terrorist act;
d) collecting and holding with the view of transmission or making available data and information on objectives targeted by terrorists, without right;
e) promoting ideas, beliefs or attitudes with the view of supporting the cause and/or the activity of a terrorist entity;
f) money laundering, fraudulent bankruptcy, corruption acts, blackmail, trafficking in human beings, illicit trafficking in drugs and precursors, contraband, trafficking in stolen vehicles, counterfeiting of currency or other valuables and any other offences with the view of obtaining a profit for the use of a terrorist entity;
g) any other acts committed with the intention of supporting, facilitating, concealing or determining the commission of terrorist acts.
The acts in para.(1) shall be punished as follows:
a) by imprisonment from 10 to 15 years and the interdiction of certain rights, for those in a) and b);
b) by imprisonment from 5 to 10 years and the interdiction of certain rights, for those in c), d) and e);
c) by imprisonment from 1 to 5 years and the interdiction of certain rights, for those in g).

For the offences provided in para.(1) f), the maximum of the punishment provided in the legislation in force shall be increased by 3 years, while not exceeding the general maximum of the punishment of imprisonment.

It shall be a terrorist act, if committed in the conditions of article 2, also the deed of a person who:
a) takes charge of a ship or fixed platform or exercises control over these through violence or threat of violence;
b) commits an act of violence against a person who is on board a ship or a fixed platform, if these acts are likely to compromise the safety of that ship or fixed platform;
c) destroys a fixed platform or a ship or causes damage to the fixed platform or to the cargo of a ship, if this is likely to compromise the safety of that platform or of the navigation of that ship;
d) places or causes to be placed on a ship or on a fixed platform, by any means, a device or a substance that is able to destroy them or to cause to the platform, to the ship or to the cargo damages that compromise or are likely to compromise the safety of that platform or of the navigation of that ship;
e) destroys or seriously damages a fixed platform or navigation installations or services or causes serious disturbance in their functioning, if one of these acts is likely to compromise the safety of the fixed platform or of the navigation of a ship;
f) communicates a piece of information in awareness that it is false, and through this compromises the safety of the navigation of a ship;
g) injures or kills any person, if these acts are related to one of the offences in a)-f).

The acts in para. (1) shall be punished as follows:
a) for the offences in a)-e) and g), by imprisonment from 15 to 25 years and the interdiction of certain rights;
b) for the offence in f), by imprisonment from 10 to 20 years and the interdiction of certain rights.

Attempt shall be punished.

The production or acquisition of means or instruments, and the taking of measures in view of committing the offences in para. (1) shall be considered attempt.

The deed of a person who leads a terrorist entity shall be punished by life imprisonment or severe detention from 15 to 25 years and the interdiction of certain rights.

The act of associating or of initiating the creation of an association with the view of committing terrorist acts or of joining or in any form supporting such an association, shall be punished by imprisonment from 10 to 15 years, while not exceeding the maximum of the punishment provided in the law for the offence that was the purpose of the association.

Making available to a terrorist entity movable or immovable assets, in awareness that they are being used for supporting or committing terrorist acts, and acquiring or
collecting funds, either directly or indirectly, or performing any financial-banking operations, with the view of financing terrorist acts, shall be punished by imprisonment from 15 to 20 years and the interdiction of certain rights.

(2) Movable or immovable assets made available to a terrorist entity, and the funds acquired or collected with the view of financing terrorist acts shall be confiscated, and if they cannot be found, the convicted shall be obliged to the payment of their equivalent in money.

– (1) The act of threatening a person or a community, by any means, with the spreading or use of products, substances, materials, microorganisms or toxins that are likely to jeopardise the health of people or animals or the environment is an offence and shall be punished by imprisonment from 2 to 5 years.

(2) The deed of threatening a state, an international organisation or a natural or legal person with the use of biological weapons, nuclear materials, other radioactive materials or explosives, in a terrorist purpose, is an offence and shall be punished by imprisonment from 3 to 12 years.

(3) If the deed provided in para.(2) is conditioned by the accomplishment or non-accomplishment of an act or if by threat, in any form, the giving or handing over of such materials is claimed, the punishment shall be imprisonment from 5 to 15 years and the interdiction of certain rights.

– The alarming, without a justified reason, a person or the public, the bodies specialised for intervention in case of danger or the bodies that maintain public order, through correspondence, telephone or any other means of remote transmission, with regard to the spreading or use of products, substances, materials, microorganisms or toxins likely to jeopardise the health of people or animals or the environment, shall be punished by imprisonment from 1 to 3 years.

– The act of a person who administers, in awareness, assets that belong to terrorist entities, on his own behalf, by concealment or by transfer to other persons, or who in any way supports such deeds, is an offence and shall be punished by imprisonment from 2 to 7 years and the interdiction of certain rights.

Crimes against the security of the state, provided in Penal Code:

- Treason
- Treason by helping the enemy
- Treason by transmission of state secret
- Hostile actions against state
- Espionage
- Attempt which jeopardize the security of state
- Attempt on a community
- Hostile acts against state power
- Diversion acts
- Hostile acts against national economy
- Propaganda for a totalitarian state
- Actions against constitutional order
- Conspiracy
- Compromising the state’s interests
- Communication of false information
- The disclosure of secret that jeopardize state security
- The omission of denunciation
- Crimes against a foreign state representative

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]

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).

Law 506/2004 concerning the processing of personal data and protection of private life in electronic communication sector allows in art.4 paragraph 2 the storage of data for purposes other then the investigation, detection and prosecution of serious crime, in the following cases:
- If it is realised by users who participates on that communication
- If the users who participates on that communication gave their previous consent in writing regarding these operation of acquisition of data.

1.A.1.e.4 Assessment of the data to be retain

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

No, the national law does not require other categories of data different from the data contained in art. 5 of the Directive. The art. 3 paragraph 1 from Law 298/2008 strictly provides the categories of data which will be retained the same with those from the Directive and art.11 paragraph 2 shows that the providers should retain only the categories of data mentioned on art.3 (1) from Law 298/2008.

1.A.1.e.4 Adequacy and law enforcement relevance of the data retained under Article 5 of the Data Retention Directive
Please indicate whether the data 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 requested to motivate their answer and provide examples of situations that demonstrate the redundancy or the flaw.
We think
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; what are typical request profiles (i.e. typical content of a request, for instance: provide a chronological listing of calls from or to a certain subscriber number, provide an overview of the relations between numbers of users or subscribers; provide statistics about the number of calls and about peaks in communication to and from a destination)? Please provide information about the type of search parameters (information selection criteria) contained in the request, 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.

1.A.1.f.2 Did your country standardise the interaction with communications service providers? If so, please provide information about the standard (form or format) for requests, the message format, the technical modalities and/or interface.

1.A.1.f.3 Please provide quantitative information about the use of the different request profiles (number or percentage/ratio of a given search profile as part of the total number of requests stated under 1.A.1.a. [Quantitative Reply]

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

1.A.1.h Does the national law governing the acquisition of communication data enable the public authority to specify the time period within which data must be disclosed, as referred to 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.

The national law, L. 298/2008, provide in art. 15 that the communications providers should transmit to public authorities, on their request, the retained data without delay, but it does not exist a specific term.

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?

There is no sanction for the fact that the providers does not respect the term in which they should transmit the retained data. There is no specific term, but it is provide that the data should be transmitted „without delay‟.

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.
The national law does not distinguish between time periods within which is required the disclosure of data by communication providers and the type of request or type of data.

1.A.1.i  Reimbursement of costs

1.A.1.i.1 Does your country reimburse CAPEX\(^1\) 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.

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.

National Law, L 298/2008 provides in art. 3 paragraph 3 provides that the cost related to the creation and administration of data base for providers are fiscal deductible.

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 allow to solve crimes that would not have been solved otherwise. It so, please provide examples [can entail Quantitative elements]

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

1.A.1.j.3 Did your Country set law enforcement targets (priorities) to achieve within a given period? If so, what is the contribution that is being made by the use of retained data in relation to achieving these targets? What is the degree of cost-effectiveness when comparing the cost for obtaining and processing retained data and the achievement of law enforcement results? How can cost-effectiveness be increased? [entails Quantitative elements]

\[^1\] CAPEX or CAPlital EXPenditure, are expenditures creating future benefits. In concrete terms it is the cost of developing or providing non-consumable parts for the product or system, and may also include the cost of workers and facility expenses such as rent and utilities.

\[^2\] OPEX or OPerational EXPenditure are operating costs or recurring expenses which are related to the operation of a business, or to the operation of a device, component, piece of equipment or facility.
1.A.2 National and transnational requests and answers

1.A.2.a For the sake of this questionnaire, "transnational requests" a distinction is made between two types of cross-border requests: 1. requests issued by law enforcement authorities from other Countries to provide data retained by service providers in your country (incoming requests) and 2. requests addressed by your country to authorities of other Member States (outgoing requests). Having regard to the total number of requests mentioned under section 1.A.1.a:

1.A.2.a.1 how many (a) incoming and how many (b) outgoing transnational requests are processed by your country on an annual basis [Quantitative Replies]

1.A.2.a.2 what is the ratio between national and transnational requests (total number of transnational requests)? [Quantitative Reply]

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]

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]

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

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?

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.

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?

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.
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?

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? Which tasks are assigned to which authority?

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

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?

1.A.3.a.4 Does any authority collect data about the economic effects of measures required under the Directive. 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]

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]

1.A.3.b 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] Centralised storage of data by Service providers

1.A.3.b.1 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]
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? Please provide a description of these measures.

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.

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 relevent means or measures [may entail Quantitative elements].

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

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]

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

1.B.1.e 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?

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

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

1.B.2.c Did the authority mentioned in the previous question investigate any cases of non-compliance with national means or measures? Please provide details, if relevent. [can entail Quantitative elements]

2 QUESTIONS TO THE EUROPEAN PARLIAMENT AND CIVIL SOCIETY

2.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

2.A.1 Which has been the effect on civil liberties of the use of data retained under the Directive?

2.A.2 Which additional measures (administrative, technical, legal, or other) would be appropriate of offset the negative impact(s)?

2.A.3 Which ones of the measures mentioned under 2.A.2 should be addressed at the level of the European Union?

2.A.4 Should the balance between enhancing security by means of retaining communication data and protecting civil liberties been stricken in a different manner. If so, please provide details how to ensure a better balance as well as the motivation underlying the policy choice. [can entail Quantitative elements]

2.B Evaluation of the effectiveness of existing (non-)legislative measures or technical solutions to ensure the traceability of users of communications services, in particular mobile phone lines, opened with prepaid SIM cards.

2.B.1 Which has been the effect on civil liberties of measures taken at national level to increase the traceability of users?

2.B.2 Which additional measures (administrative, technical, legal, or other) should be taken of offset the negative impacts?

2.B.3 Which ones of these measures should be addressed at the level of the European Union?

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

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 10Please provide information on the distribution of competences of supervisory authorities according to Directives 95/46/EC, 2002/58/EC and 2006/24/EC.

Directive 95/46/EC of the European Parliament and Council has been transposed into Romanian legislation through Law no. 677/2001 on the protection of individuals with regard to the processing of personal data and the free movement of such data, adopted on the 12th December 2001, as modified and amended.

In the terms of Law no. 677/2001, modified and completed, the supervisory authority is the National Supervisory Authority for Personal Data Processing.

The supervisory authority carries out its activity completely independent and impartial.

The supervisory authority shall monitor and control with regard to their legitimacy, all personal data processing, subject to this law. In order to achieve this purpose, the supervisory authority exerts the following attributions:

a) issues the standard notification forms and its own registers;

b) receives and analyses the notifications concerning the processing of personal data and informs the data controller on the results of the preliminary control;

c) authorizes personal data processing in the situations set out by law;

d) may dispose, if it notices the infringement of the provisions of the present law, temporarily suspending the data processing or ending processing operations, the partial or total deletion of processed data and may notify the criminal prosecution bodies or may file complaints to a court of law;

d) 1) informs the natural or legal persons that work in this field, directly or through their associative bodies on the need to comply with the obligations and to carry out the procedures set out by this law;

e) keeps and makes publicly accessible the personal data processing register;

f) receives and solves petitions, notices or requests from natural persons and communicates their resolution, or, as the case may be, the measures which have been taken;

g) performs investigations –ex officio, or upon requests or notifications;

h) is consulted when legislative drafts regarding the individual’s rights and freedoms are being developed, concerning personal data processing;

i) may draft proposals on the initiation of legislative drafts or amendments to legislative acts already enforced, in the fields linked to the processing of personal data;

j) collaborates with the public authorities and bodies of the public administration, centralizes and analyzes their yearly activity reports on the protection of individuals with regard to the processing of personal data, issues recommendations and assents on any matter linked to the protection of fundamental rights and freedoms regarding the processing of personal data, on request of any natural person, including the public authorities and bodies of public administration; these recommendations and assents must mention the reasons on which they are based and a copy must be transmitted to the Ministry of Justice; when the recommendation or assent is requested by the law, it must be published in the Official Journal of Romania, Part I;

k) co-operates with similar foreign authorities in order to ensure common assistance, as well as with foreign residents for the purpose of guaranteeing the fundamental rights and freedoms that may be affected through personal data processing;

l) fulfills other attributions set out by law;
Directive 2002/58/CE on the processing of personal data and the protection of private life within the electronic communications' sector has been transposed into national law through Law no. 506/2004 on the processing of personal data and the protection of private life within the electronic communications' sector, as modified and completed.

According to Law no. 506/2004, corroborated with Law no. 677/2001, modified and completed and Law no. 102/2005 regarding the setting up, organization and functioning of the National Supervisory Authority for Personal Data Processing, the authority, through it’s empowered control personnel, is competent to ascertain contraventions, explicitly set out by Law no. 506/ and to apply sanctions.

Directive 2006/24/CE of 15th March 2006 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 of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector has been transposed into national law in Romania through Law no. 298/2008 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks, as well as on amending Law no. 506/2004 on the processing of personal data and the protection of privacy in the electronic communications sector. Law no. 298/2008 has been declared as unconstitutional by the Romanian Constitutional Court.

3.A.1 Do authorities have investigative powers vis-à-vis providers and have there been any cases of complaints etc that have led to supervisory or investigative activities?

According to the provisions of Law no. 677/2001, as modified and amended, as well as to those Law 506/2004, the supervisory authority has investigative attributions as regards the suppliers, personal data controllers.

We would like to mention that during the time Law no. 298/2008 was in force, the supervisory authority hasn’t received any complaints related to the provisions of this legislative act.

3.A.2 Do authorities have investigative powers vis-à-vis public authorities and have there been any cases of complaints etc that have led to supervisory or investigative activities?

According to Law no. 677/2001, modified and completed, this law applies to the processing of personal data, carried out by Romanian or foreign natural or legal persons of public or private law, regardless of the fact that the data processing takes place in the public or private sector. Thus, the supervisory authority has investigative attributions also as regards public authorities.
Complaints have been registered within the activity of the supervisory authority as regards the activities of public authorities as data controllers; however these haven’t referred to the enforcement of the legislative act that implemented Directive 2006/24/EC.

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. [can entail Quantitative elements]

Which According to Law no. 677/2001, the supervisory authority shall monitor and control with regard to their legitimacy, all personal data processing, subject to this law.

The National Supervisory Authority for Personal Data Processing has carried out investigations on the compliance at national level of phone and internet services’ providers with the obligations imposed by national law on data retention, based on articles 6 and 9 of the Directive on the processing of personal data and the protection of privacy in the electronic communications sector 2002/58/EC and the data retention Directive 2006/24/EC, which amends Directive 2002/58/EC.

The investigations’ main purpose was to analyze whether the requirements on data protection as regards the type of data retained, the security measures, the prevention of abuses and the obligations on the limits of storage within the telecommunications’ sector.

Within this context, a representative sample of national telecommunications’ providers was selected, based on the market share, type of services provided at the national, European or international span of the company (providers of fixed and mobile telephony and internet)

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

In view of the findings of the investigations carried out by the supervisory authority in the period Law no. 298/2008 has been into force, it may be ascertained that the providers of electronic communication services and networks did not ensure in an unitary way the management of the retention and process of data, even though they have tried to comply with the requirements of the legislative act on data retention.

3.A.5 Do authorities have experience 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]

N/A
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?

Directive 2006/24/CE of 15th March 2006 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 of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector has been transposed into national law in Romania through Law no. 298/2008 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks, as well as on amending law no. 506/2004 on the processing of personal data and the protection of privacy in the electronic communications sector. Law no. 298/2008 has been declared as unconstitutional by the Romanian Constitutional Court.

Law no. 298/2008 through which Romania has transposed the provisions of Directive 2006/24/EC has been declared unconstitutional by the Romanian Constitutional Court through its Decision no. 1258 of the 8th October 2009.

3.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.

N/A

3.B.1 Please provide details of the observations made by the data protection authorities with regard to practical needs and privacy issues concerning the traceability of users, in particular of mobile pre-paid SIM cards. In case any procedure has been brought against the such means or measures deployed in your country, please provider details about this procedure. [can entail Quantitative elements]