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]

In 2008, total number of requests was 4490.

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]

In 2008, percentage of requests generated by type of requesting authority in 2008 was following:
1. police – 97%
2. judicial – 2%
3. other authorities (Tax and Customs Board) - 1%

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 average age of the data that is requested is between 0...3 months.

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.

In principle, the exchange of information can be done either electronically or in written form (as stipulated in the Electronic Communications Act § 112). In practice, exchange of information with all significant operators is done electronically and with smaller companies in written form. The information which has been classified as not urgent shall be forwarded by e-mail. For the exchange of information with the large communication companies, the relevant secure electronic network has been established by which the police can produce
inquiries electronically. It has been established by the communication companies themselves.

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

According to the Estonian legislation, the inquiry concerning the electronic communication service shall be qualified as surveillance activity. To collect evidences by surveillance activities is allowed only in the cases if the subject of the criminal proceeding is the crime of the first degree or the crime of the second degree committed with the intent and for what the imposed punishment is at least three years imprisonment.

The Criminal Procedure Code §110 (admissibility of surveillance activities in collection of evidence) declares that:

1) Evidence may be collected by surveillance activities in a criminal proceeding if collection of the evidence by other procedural acts is precluded or especially complicated and the object of the criminal proceeding is a criminal offence in the first degree or an intentionally committed criminal offence in the second degree for which at least up to three years’ imprisonment is prescribed as punishment.

1') Evidence may be collected by the surveillance activities specified in § 117 of this Code as a single inquiry on the conditions provided for in subsection (1) of this section in criminal proceedings commenced pursuant to § 120, 156, 157, 179 and 180, subsection 206 (1), § 207, subsection 208 (1), subsection 217 (1), §§ 245, 247, 249, 275, 305 and 323, subsection 377 (1) and § 398 of the Penal Code. For the purposes of this section, single inquiry is an inquiry for obtaining the information specified in subsection 117 (1) concerning a particular telephone call, a particular electronic mail, a particular electronic commentary or another communication session related to the forwarding of a single message.

List of crimes (in the Estonian Penal Code) in which the acquisition and use of retained data is allowed is following:

§120 - Threat
§156 - Violation of confidentiality of messages
§157 - Violation of obligation to maintain confidentiality of secrets which have become known in course of professional activities
§179 - Sexual enticement of children
§180 - Exhibiting violence to minors
§206(1) - Interference in computer data
§207 - Hindering of operation of computer system
§208(1) - Dissemination of spyware, malware or computer viruses
§217(1) - Unlawful use of computer system
§245 - Defamation of official symbols of Republic of Estonia
§247 - Defamation and insulting of persons enjoying international immunity
§249 - Defamation of official symbols of foreign state or international organization
§275 - Defamation or insult of representative of state authority or other person protecting public order
§305 - Defamation and insulting of court or judge
§323 - Violation of confidentiality requirement
§377(1) - Unjustified disclosure and use of business secrets
§398 - Abuse of inside information

The main crimes when the inquiries shall be implemented are related to drugs, crimes against

[1] Collection of information concerning messages transmitted through commonly used technical communication channels
person and economic crimes (serious crimes).

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]

Estonia does not gather statistics related to the average age of the data that has been requested for the different types of crime and it is why there is no statistic analysis concerning such kind of data.

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.

No, the national law does not allow 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. According to the Estonian legislation, the data described in the Directive are not allowed to be used for other purposes than to collect evidences in the criminal proceedings.

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.

No, only the data that is set out in Article 5 of the Directive must be retained. In Estonia, the data not being described in the Directive shall not require retention.

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.

In our opinion data retained under Articles 5 is sufficient, however, the question of efficiency needs additional evaluation due to the fact that some parts of the DR Directive were integrated in our national law quite recently (in April 2009).

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.
The typical search parameters contained in requests for the acquisition of retained data are the owner of certain telephone number; location address of subscriber; communication made from or to a given phone number; the usage of IP address at certain 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.

No, but further analysis is possible.

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:

In case of urgent request the data must be disclosed without undue delay, but within 10 hours. Non-urgent requests must be answered within 10 working 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.

N/A.

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?

If necessary, to ensure the respect of the time period within which they request the reply to be given, supervision can be carried out.

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. But see also answer 1.A.1.h

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.

The communication companies provided with the electronic network to exercise inquiry, shall

---

\(^1\) CAPEX or CAPital Expenditure, are expenditures creating future benefits. In concrete terms it is the 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.
receive compensations to cover the costs concerning the surveillance activities. Reimbursement for updating is linked to the size of the procedure and it is solved through the negotiations between the parties to reimburse or not.

According to §114 (1) of the Electronic Communication Act the communication company’s costs shall be compensated that are related to the transmission of messages prescribed by the § 112 of the Electronic Communication Act to the surveillance agency or the data described in the Directive. The costs shall be compensated from the state budget through the budget of ministry in the area of government (Ministry of the Interior) of which the surveillance agency or security authority belongs.

1.A.1.1.2 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.

Pursuant to §114 (4) of the Electronic Communication Act the costs are compensated in accordance to the contract entered into between the surveillance agency or security authority and the communications undertaking and where services, fees, costs of inquiry and other conditions shall be established. The contract and the contract conditions shall not be revealed to the third parties.

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]

The data acquired under the Directive is not and cannot be exclusive evidence to detect or prosecute a crime. In Estonia, the data can only be acquired, if all other measures of criminal procedure have failed (§ 110 Art 1 in the Code of Criminal Procedure), thus the data is never a sole pillar of detection or prosecution. The evidence cannot be weighted beforehand and has to be regarded as a whole. This means, that law-enforcement agency does not hold statistics, which evidence (phone billing, eyewitness account, DNA-evidence etc) was the most helpful part of detection in the sense that this could be quantitatively presented after. We would like to draw attention to the fact that law enforcement agencies do not have unlimited resources and a measure that is not effective from the standpoint of detection/prosecution tends to be used less. As the number of data requests is significant it has been proven to be a useful tool in law enforcement.

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]

N/A.

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

N/A.

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]

1.A.2.a.4 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]

Within the reasonable time.

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]

Within the reasonable time.

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

Direct consultations 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?

The Prosecutor’s Offices and courts with cooperation of Ministry of Justice take the decision to issue 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.

Central authority for forwarding request for judicial assistance is 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?

No.

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.

Estonia accepts requests in Estonian or in English.

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?

All requests incoming to Ministry of Justice are expected to be already translated to the correct language. Ministry of Justice has only limited resources for translations in the field of responsibility.

1.A.2.g  Data security

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

The Public Prosecutors Office as being in charge of criminal matters shall direct pre-trial proceedings and ensure the legality and efficiency thereof. In the case of the Security Police Board, also the Parliaments Special Committee of Security Authorities has the right to control the legality of the activity of SPB.

There are general requirements to ensure data protection and access procedures according to the directive 2002/58/EC. In fact, communication undertakings are having strict rules for access to data and all requests are logged.

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?

National authorities charged with tasks resulting from the Directive are:
- Ministry of Economic Affairs and Communications (preparation of legislation, assessing economic impact, surveillance) and
- Estonian Technical Surveillance Authority (surveillance).

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

The respective authorities are operational since adoption of the Directive.
1.3.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?

Ministry of Economic Affairs and Communications - no reorganization is needed nor staff. The personnel only got some new tasks related to the Directive.

1.3.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]

No, data about the economic effects of measures required under the Directive is not collected.

1.3.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]

No.

1.3.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. [lastpar may entail Quantitative elements]

No.

1.3.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]

No, we are not aware of such problems.

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 (cf 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.

At the moment, Estonia does not have any comprehensive legal framework in order to increase the traceability of prepaid SIM-cards. The information listed in question above can be obtained through criminal procedure. Various methods are used for identifying the owners of prepaid cards, including surveillance measures which are not limited to surveillance activities performed in telecom (e.g. loading the card from the bank account).

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.

The collection of information concerning the users of the mobile phones is regulated by the Code of Criminal Procedure, the Surveillance Act, and the Electronic Communications Act, which are at the moment sufficient for ensuring the availability of data. The gathering of information about telephones is according to Estonian laws usually a surveillance activity and it can only be performed in the case of surveillance investigation, which can in turn be instigated for the detection of those crimes that are punishable by at least a 3-year imprisonment. Such crimes are usually related to drug crimes, crimes against the person, crimes against property, and economic crimes.

1.B.1.e Efficiency

1.B.1.c 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].

Please see answer to question 1.A.1.j.1.

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

N/A.

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]

N/A.

1.B.1.c.4 What are the costs or these measures for the private sector? [can entail Quantitative elements]
Costs are depending on the existing technical capabilities. Some of operators had almost no costs because existing network management software already was in some way capable of retaining data. Some bigger operators, who are having secure online query channels with police and other authorities, had to make investments about 500,000 EUR.

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?

The implementation of measures to increase traceability has to be done on EU level as it affects both internal security and fair competition. Having said that, Estonia is currently analyzing the effects of the data retention Directive in force and thus it would be premature to present challenges and concrete solutions to the problems.

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?

Law enforcement authorities have conducted regular internal trainings and seminars where the procedures to obtain intelligence from the databases of the communication companies and the requirements provided by the law and other conditions obligatory for performance of the inquiry have been introduced.

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 have been no studies on that issue.

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

Yes.

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]

If non-compliance is detected, a case investigation will be carried out.

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?

There is no obligation to identify prepaid SIM card users.
3 Questions addressed to National Supervisory 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 1. Please provide information on the distribution of competences of supervisory authorities according to Directives 95/46/EC, 2002/58/EC and 2006/24/EC.

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.

Estonian DPA has investigative powers vis-à-vis providers regarding the Electronic Communications Act § 102 (A communications undertaking is required to maintain the confidentiality of all information which becomes known thereto in the process of provision of communications services and which concerns subscribers as well as other persons who have not entered into a contract for the provision of communications services but who use communications services with the consent of a subscriber; above all, the following data must be protected: specific data of using communications services; the content and format of messages transmitted through the communications network; information concerning the time and manner of transmission of messages) within the limits of competence provided by the Personal Data Protection Act. There has not been any cases of complaints that have led to supervisory or investigative activities.

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.

Estonian DPA has investigative powers vis-à-vis public authorities within the limits of competence provided by the Personal Data Protection Act. There hasn’t been any complaints that have led to supervisory or investigative activities.

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]

Estonian DPA has the power to audit the compliance of providers regarding the Electronic Communications Act § 111.1 (data retention obligation) and the Personal Data Protection Act. No audits have been carried out at the moment, but the Estonian DPA is planning on-site inspections amongst the providers in the near future.

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 as Estonian DPA has not carried out any audits, there is no knowledge of the practical implementation of the Directive.

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 this context and the approach that has been followed to settle the Contentious issues, [can entail Quantitative elements]
Estonian DPA has no experience with the supervision of data that service providers have stored centrally.

3.6 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 as there has not been any case law regarding the implementation or use of the Data Retention Directive or the use of retained data.

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. Please provide details of the observations made by the data protection authorities with regard to practical needs and privacy issues surrounding measures intended to increase the traceability of users, if any, in particular of mobile pre-paid SIM cards, in particular from the point of view of ensuring the appropriate balance between the respect the privacy of users and security interests. 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]

N/A as evaluation of the effectiveness of existing (non-)legislative measures or technical solutions is in the competence of Estonian Technical Surveillance Authority.
4 **QUESTIONS TO THE PRIVATE SECTOR f ISPS, TELECOM OPERATORS, NETWORK AND CABLE OPERATORS**

N/A.

4.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.

*For all questions in this section, please differentiate by type of service if applicable*

4.A.1 Does the implementation of the Directive have the effect of requiring communication providers to retain data for a longer period than permitted for business purposes under Directive 2002/58/EC?

4.A.2 Do national authorities oblige communication providers to retain data, e.g. regardless of size, customer type and number, type of service? If national authorities differentiate between private sector stakeholders, please describe the criteria for such differentiation.

4.A.3 Since when are data retention obligations in force, and, where relevant: since when is data retention applied in practice within a specific Member State with regard to specific communication providers?

4.A.4 Please provide details about the investment costs, if any, to fulfil their obligations on:

*AAA.a* retaining the data for the period required by national law,

*4.A.4.b* ensuring the security requirements imposed by the Directive,

*4.A.4.C* responding to requests without "undue delay", as defined by national law or in a service level agreement.

*4.A.4.d* ensuring that data are only retained for the purposes defined in the Directive and separated from data used for business operations, as determined by national law and necessary.

4.A.5 Please provide details about the implementation of specific organisational measures and procedures, if any, by communication providers that are necessary to comply with the obligations identified in the previous question (a-d)?

4.A.6 Is it possible to quantify financial impacts of the necessary measures? If so, please provide the relevant information to assess this impact [can entail Quantitative elements]

4.A.7 Does the reimbursement by national authorities, if any, cover the expenditure necessary for compliance with the Directive?

4.A.8 Does the relevant legislation and practice provide providers with legal certainty regarding their obligations concerning the protection of data of their subscribers and users?

4.A.9 Have providers received direct requests from authorities in another Member State than that of their establishment? Were their any problems with these requests? If so, please provide a description of these problems.
4.A.10 Please provide information, differentiated by type of operator etc concerning the elements of section I.A.1 of this questionnaire.

4.A.11 Which economic effect do providers observe

4.A.11.a on competition,

4.A.11.b investment in new infrastructures and services,

4.A.11.c retail tariffs? Please provide quantitative information, and where such is not possible, qualitative indicators to allow assessment of the economic effect.

4.A.12 Centralised storage of retained data

4.A.12.a Do operators store data at a centralised level outside of the country where the data are generated? If so please provide details about the location, size and business impact of the centralised storage

4.A.12.b Do operators transfer retained data that are stored at centralised level to other countries that are bound by the Data Retention Directive or to third countries?

4.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

4.B.1 Please provide information about the number of cases where communication providers been requested to identify users of pre-paid SIM cards?

Which means do providers have to identify users of prepaid SIM cards? Please describe the number of cases or ratio of cases where information could not be provided in relation to the means used.