Latvijas Republikas Pastāvīgā pārstāvniecība Eiropas Savienībā
Permanent Representation of the Republic of Latvia to the European Union

23, Avenue des Arts, 1000 Brussels tel. (32 2) 238 31 00 fax (32 2) 238 32 50, e-mail: permrep.eu@mfa.gov.lv

Briselē, 2010.gada 26.janvārī
Nr.2.3.6 - 227


Joaquim Nunes de Almeida
Tiesiskuma, brīvības un drošības ģenerāldirektorāta
F direktorāta F3 nodaļas vadītājs
Eiropas Komisija

Par atbilstu sniegšanu uz aptaujas anketu


Pielikumā: tekstā minētās atbildes uz aptaujas anketu uz 23 lpp.

Ar cieņu,

Normunds Popens
Pastāvīgais pārstāvis

DG JLS/CAD
01.02.2010
1593
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.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]

Reply to 1.A.1.a:
Total number of the requests is attached in the annex.

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]

Reply to 1.A.1.b:
In accordance with the Section 19 (1) lit.15 of Electronic Communications Law the electronic communications merchants have a duty once per year provide statistical information to the State Data Inspection regarding the applications from the institutions referred to in Section 71.1, Paragraph one of this Law (including the State Security institutions) to receive retained data and regarding the issuing of such data do not indicating the institutions, which has requested the data.

The legislation of Latvia does not obligate the law enforcement authorities to count the requests, wherewith we do not have precise information about the count of the requests, which were made by the law enforcement authorities regarding the requirements of the Directive 2006/24/EC.

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]

Reply to 1.A.1.c:
The reply on this question is included in the reply to the question No. 1.A.1.a.

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

Reply to 1.A.1.d:
Mostly there are used the written documents and the form of the delivery of these documents is by post, courier. Also documents are delivered by e-mail.

Type of crimes

1.A.1.d.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

Reply to 1.A.1.e.1:
In accordance with the Section 71.1 of Electronic Communications Law the duty to retain and transfer data refers to all authorities who provide the disclosing, investigation and prosecution of crime, including the State security institutions.

Wherewith Electronic Communications Law does not divide the particular crimes under Criminal Law of Latvia.

1.A.1.d.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]

Reply to 1.A.1.e.2:
In accordance with the Section 19 (1) lit.15 of Electronic Communications Law electronic communications merchants have a duty to provide statistical information to the State Data Inspection do not indicating the institutions, which has requested the data.

The legislation of Latvia does not obligate a duty to provide statistical information regarding retained data depending from the type of crime wherewith we do not have precise information.

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

Reply to 1.A.1.e.3:
The Civil Procedure Law (Article 112 and 120 of the Civil Procedure Law) and Administrative procedure Law (Article 150 (4) and 177 of the Administrative procedure Law) authorizes the court to require any proof if it is necessary to determine the facts in a matter.

According to the above mentioned laws it is not prohibited to request the data mentioned in the Article 5 of the Directive No. 2006/24/EC.

In addition we would like to stress that request of any data mentioned in the Article 5 of the Directive No. 2006/24/EC in the civil procedure or in the
The Regulations of the Cabinet of Ministers No. 820 of 4th December 2007 “Procedures by which Pre-trial Investigative Institutions, Bodies Performing Investigatory Operations, State Security Institutions, Office of the Prosecutor and Court Request and a Merchant of Electronic Communications Transfers Data to be Retained, and Procedures by which Statistical Information regarding Requests of Data to be Retained and Issuing thereof is Compiled,” issued pursuant to Section 71.1, Paragraphs four and five of the Electronic Communications Law states:

“10. A merchant of electronic communications shall ensure submission of the data to be retained within the following time periods after the receipt of a request:

10.1. within 30 days, if such data are requested, which were retained more than six months ago;

10.2. within 10 days, if such data are requested, which have been retained during the last six months;

10.3. in matters of urgency, if the transfer of data within the time period referred to in Sub-paragraphs 10.1 or 10.2 may hinder the prevention or disclosure of a criminal offence, saving a person's life or protection of the State or public safety (hereinafter – matter of urgency) – within three hours, if the data requested have been retained within a time period of the last twenty-four hours; and

10.4. in matters of urgency, if the data referred to in Paragraphs 1, 2 and 3 of Annex 1, Paragraphs 1, 9, 10 and 13 of Annex 2 or Paragraphs 1 and 2 of Annex 3 to these Regulations have been requested – within an hour.

11. If due to technical limitation reasons it is not possible to ensure transfer of the data to be retained within the time periods referred to in Paragraph 10 of these Regulations, a merchant of electronic communications shall inform thereof the relevant authority, the Office of the Prosecutor or court, and the requested data shall be submitted without delay, as soon as possible.”

1.A.1.g.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?

Reply to 1.A.1.h.2:

If the electronic communications merchants do not provide with data and there is a base to consider that the electronic communications merchants have required data in this case in accordance with the Criminal Procedure Law the measures of compulsion (for example, seizure, searches) can be used.

Depending of the facts in matter in the case of failure to comply in good time with the lawful requests of officials of State or local government institutions exercising control, supervision or investigatory functions accordance with the Section 175.2 of Latvian Administrative Violations Code administrative punishment could be applied to the electronic communications merchants.

1.A.1.g.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.

5
Reply to 1.A.1.h.3:
The answer to this question is included in answer to question No. 1.A.1.h.1.

1.A.1.h Reimbursement of costs

1.A.1.h.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.h.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.

Reply to 1.A.1.i.1-1.A.1.i.2:
There is no reimbursement of costs.

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

1.A.1.i.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]

Reply to 1.A.1.j.1:
We do not select information about the importance of data in issue of detection and prosecution of crimes. Practical experience shows that retained data assist in detection and prosecution of crimes. Retained data can be considered as evidence in criminal procedure.

1.A.1.j.1 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]

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

Reply to 1.A.1.j.2 - 1.A.1.j.3:

---

\(^1\) CAPEX or CAPital 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.
administrative procedure could be restricted by conditions to be proven in connection with the actions of a person in the concrete case. Both the Civil procedure law and the Administrative procedure law allow acquisition of the data relating the known person.

1.A.1.d.4 Assessment of the data to be retained

1.A.1.d.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.

*Reply to 1.A.1.e.5:*
Electronic Communications Law does not require the retention of other categories of data in addition to the data contained in Article 5 of the Directive No. 2006/24/EC.

1.A.1.d.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.

*Reply to 1.A.1.e.6:*
Data retention concerns general retention for all communications of certain categories of signalling information or determined communication services for a fixed period after the end of the communication in view of use by law enforcement. Data retention is not about content (not about legal interception) and retention for specific targets at demand of law enforcement (data preservation). There are an industry and law enforcement needs to retain the particular traffic data. For e-commerce these needs include the logical protection of their infrastructure (network) and user protection / trust / confidence (is possible only with serious level of security). Serious level of security also is not possible without combating criminal abuse. The needs for law enforcement include to receive reliable information about subscriber (identify user on each level of the communication), because often it is bogus information (for example, spoofed IP or MAC, TOR or SOCKS CHAIN, abused device etc.), but the traffic data are not always available. The need for industry to retain the data is connected, for instance, with Intellectual property industry, when it is impossible to obtain the data on suspects of piracy.

According to the Article 5 of directive 2006/24/EC, there are only two types of Internet services, which communication data is preserved (Internet e-mail and
Internet telephony). Unfortunately, this mentioned article does not cover other types of services, such as instant messaging, web publishing, file transfer, P2P networks etc. So we propose to expand these services, which communication data is necessary to retain.

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

1.A.1.e.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.

Reply to I.A.1.f.1:

The legislation of Latvia does not oblige to summarize information on the criteria of selection. The practical experience shows that these criteria are: identifying data of the subscriber, the incoming and outgoing calls of the telephone, the telephone number of subscriber, international mobile equipment identity (IMEI), international mobile equipment location identity, Internet protocol (IP) address.

1.A.1.e.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.

Reply to I.A.1.f.2:

Till today we have not standardised the format for the acquisition and disclosure of communications data. At the same time some of the law enforcement authorities are planning to make arrangements with the electronic communications concerning exchange of information of retained data through Internet.

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

1.A.1.g 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.g.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.

Reply to I.A.1.h.1:
During the detection and prosecution of crimes the costs of using the retained data are not carried out.

1.2 National and transnational requests and answers

1.2.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:

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

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

Reply to 1.2.a.1 – 1.2.a.2:

Retained data from the EU member states as well as from the third countries is processed on the basis of received mutual legal assistance requests or using co-operation facilities of Europol or Interpol. Basically retained data is requested in connection with concrete investigations. Retained data is only a part of information that is requested in the framework of mutual legal assistance requests. There is no statistical information on this issue.

Having regard to the total number of requests mentioned under section 1.2.a.1:

1.2.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]

1.2.a.4 what is the ratio between national and transnational requests (total number of transnational requests)? [Quantitative Reply]

Reply to 1.2.a.3 – 1.2.a.4:

Retained data is only a part of information that is requested in the framework of mutual legal assistance requests. There is no statistical information on this issue.

1.2.b What is the average time to:

1.2.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.2.b.1)? What are the elements (for instance: type of procedure) that determine the length of the procedure? [Quantitative elements]

1.2.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?

Reply to 1.A.2.b.1 – 1.A.2.b.3:
The dates of providing of answers are determined in the Regulations of the Cabinet of Ministers No.820 (see answer to question No. 1.A.1.h.1).

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?

Reply to 1.A.2.c:
All law enforcement authorities have a right regarding their competence to make or prompt to make transnational requests.

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.

Reply to 1.A.2.d:
Requests for legal assistance in Latvia can receive the Ministry of Justice, Prosecutor General Office and State Police. The outgoing and incoming requests in issues of police cooperation can be processed using cooperation facilities of Europol, Interpol or other police mechanism of cooperation.

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?

Reply to 1.A.2.e.1:
The costs are not reimbursed.

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.

Reply to 1.A.2.f.1:
Legal assistance requests are received in national language (Latvian) if is not agreed between the parties on using of other language. In police cooperation issues is used the language foreseen by channels of police cooperation.

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?

Reply to 1.A.2.f.2:
The authority which receives the request provides the translation of the request if it is necessary.

1.A.2.g  Data security

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

Reply to 1.A.2.g:
In purpose to provide data protection there are used such measures:
1) The access rights are divided and authorization of access to workstations and to systems of information;
2) Notes of audit are performed;
3) The confidential disclaimers and internal procedure regulations, which are signed by members who start employment relationships;
4) Providing with the restriction of access to rooms where is performed the processing of data and documents are retained.

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?

Reply to 1.A.3.a.1:
Requirements resulting from the Directive are implemented in Electronic Communications Law. There are no national authorities who are charged of specific tasks resulting from the Directive. While pointing that in accordance with
the Section 8 (1) lit. 6 of Electronic Communications Law the Public Utilities Commission supervise compliance with regulatory enactments in the electronic communications sector. In accordance with Electronic Communications Law electronic communications merchants have to receive general authorisation provided by the Public Utilities Commission.

General authorisation – the rights and requirements specified in regulatory enactments for electronic communications merchants, which may include specific electronic communications sector conditions and which may be applied to all or to specific types of electronic communications networks or electronic communications services.

If the electronic communications merchant does not perform necessary requirements regarding his activity in this case the necessity of issuing of general authorisation to concrete electronic communications merchant is evaluated to concrete electronic communications merchant.

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 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]

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.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]

Reply to 1.A.3.a.2 - 1.A.3.a.6:
See question No. 1.A.3.a.1.
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]

Reply to 1.A.3.a.7:

In accordance with the Electronic Communications Law and The Regulations of the Cabinet of Ministers No. 820 of 4th December 2007 “Procedures by which Pre-trial Investigative Institutions, Bodies Performing Investigatory Operations, State Security Institutions, Office of the Prosecutor and Court Request and a Merchant of Electronic Communications Transfers Data to be Retained, and Procedures by which Statistical Information regarding Requests of Data to be Retained and Issuing thereof is Compiled” a merchant of electronic communications shall ensure submission of the data to be retained within the certain time periods after the receipt of a request.

Till today no problems have been found regarding obtaining retained data.

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

1.B.1 Law enforcement issues

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

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?

Reply to 1.B.1.a – 1.B.1.b:
The legislation of Latvia does not provide collateral duty for the electronic communications merchants to implement different measures.

If the particular electronic communications merchant processes the data regarding his own implemented measures then law enforcement authorities in accordance with the legislation obtain data thereby increasing the obtaining of information of particular person.

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].

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

Reply to 1.B.1.c.1 – 1.B.1.c.4:
As the legislation of Latvia does not provide collateral duty for the electronic communications merchants to implement different measures, we do not have precise information regarding assessment of the effectiveness of the measures.

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?

Reply to 1.B.1.d:
See question No. 1.A.1.e.6.

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?

Reply to 1.B.1.e:
Training courses about the methods of detection and investigation of crimes, including also using of retained data, are provided for personnel of law enforcement authorities on the regular basis. The specific training courses regarding use of retained data are organized by the law enforcement authorities in accordance with its competency.

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?

Reply to 1.B.2:
As the legislation of Latvia does not provide collateral duty for the electronic communications merchants to implement different means or measures, we do not have precise information regarding assessment of the impact of the means or measures on the market.

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

Reply to 1.B.2.b:
See question No. 1.A.3.a.1.

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]

Reply to 1.B.2.b.1:
In accordance with the Section 9 of Electronic Communications Law the Public Utilities Commission is assigned a number of rights which can be used to ensure the monitoring of implementation of laws. Accordance with the Section 9 of Electronic Communications Law and with the Section 215.10 of Latvian Administrative Violations Code the Public Utilities Commission has the right to apply the administrative punishment in the cases specified by law.

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?
Reply to 1.B.2.b.2: Electronic Communications Law doesn’t determine the obligatory registration of users of pre-paid SIM cards.

2 QUESTIONS ADDRESSED 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, if any, on civil liberties of the use by law enforcement authorities of data retained under the Directive? Please provide examples of these effects as well as indications of the size of their impact.

2.A.2 What additional measures (administrative, technical, legal, or other) would be appropriate for the offset of any negative impact(s) which has been identified?

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 Having regard to changes in technology and experience gathered with the operation of the Data Retention Directive, is the balance provided for by the Directive between enhancing security by means of retaining communication data and protecting civil liberties still appropriate? If a different balance is deemed to be appropriate, please provide details how to adjust the balance as well as the motivation underlying the assessment. [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 What has been the effect, if any, on civil liberties of measures taken at national level to increase the traceability of users of communication devices? Please provide examples of these effects as well as indications of the size of their impact.

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

2.B.3 Which ones of these measures should be addressed at the level of the European Union?
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 10. Please provide information on the distribution of competences of supervisory authorities according to Directives 95/46/EC, 2002/58/EC and 2006/24/EC.

*Reply to 3.A:*

In accordance with the Directive 95/46/EC in Latvia the institution of supervision is Data State Inspectorate under Article 29 (1) of Personal Data Protection Law. National authorities of supervision listed in Directive 2002/58/EC are provided in the Article 4 of Electronic Communications Law - the electronic communications sector shall be supervised by the Public Utilities Commission and the protection of personal data in the electronic communications sector shall be supervised by the Data State Inspectorate. In accordance with the Article 9 and 19 of Directive 2006/24/EC

The competent institution on summarizing the statistics is Data State Inspectorate of Latvia – it is stipulated in Section 5 of Article 71 of Electronic Communication Law.

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.

*Reply to 3.A.1:*

Data State Inspectorate can conduct an inspection on personal data processing of electronic communication providers if it doesn’t effect the retained data because Data State Inspectorate has no authorization to access retained data.

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.

*Reply to 3.A.2:*

Data State Inspectorate can conduct an inspection on personal data processing of law enforcement authorities if it doesn’t involve access to retained data, data processing in framework of Criminal Procedure Law, Investigatory Operations Law and Law on State Security Establishments. Data State Inspectorate has no authorization to access retained data.
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]

**Reply to 3.A.3:**
Data State Inspectorate hasn’t conducted the audits regarding compliance of providers, because of the Article 71 of Electronic Communications Law does not foresee the power for Data State Inspectorate to access retained data hence the complete audit is not possible.
In 2009 Data State Inspectorate has conducted the inspections in the framework of the Article 29 Working Party of Directive 95/46/EC joint investigation regarding data processing carried out by electronic service providers, however excluding the access to the retention data.

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]

**Reply to 3.A.4:**
There are such problems:

1) the authorizations to Data State Inspectorate to access to the retained data are not determined in legislation of Latvia that is the obstruction in investigation of the cases that require such information, also Data State Inspectorate can not fully take supervisory role regarding processing of the retained data in public and private sector;

2) Data State Inspectorate can not perform the inspection regarding the validity of the requests made by the law enforcement authorities to execute the data subject rights determined in Article 20 of Personal Data Protection Law regarding the appeal to the Data State Inspectorate the refusal to provide the information referred to in Article 15 of Personal Data Protection Law (in accordance with this Article data subject has the right to obtain all information that has been collected concerning himself or herself in any system for personal data processing, unless the disclosure of such information is prohibited by law in the field of national security, defence and criminal law). Because of the deficiencies of national legislation - Data State Inspectorate has no authorizations to access the retained data.

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 that context and the approach that has been followed to settle the contentious issues. [can entail Quantitative elements]
Reply to 3.A.5:
In practice of monitoring provided by Data State Inspectorate the situations are identified when the centralised data base of electronic communications service provider where the retained data are retained is located in other state of European Union. In such situations the problems were related to the access to information on organizational issues of data processing as well as problems to conduct the inspections in situ.

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

Reply to 3.A.6:
Concerning the infringements of personal data there were no precedents regarding the using of the retained data in the purpose of criminal investigation and also for the implementation of the Directive.

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 provide details about this procedure. [can entail Quantitative elements]

Reply to 3.B:
Latvian electronic communication service providers offer the pre-paid cards for telecommunication services. The Electronic Communication Law does not foresee the mandatory registration of pre-paid card users, but the telecommunication service providers have implemented such an option with the aim of identification of users. In the case of pre-paid anonymous services, the date and time of the initial activation of the service and the location label (for example, Cell ID) from which the service was activated are retained.
4 **QUESTIONS TO THE PRIVATE SECTOR (ISPs, TELECOM OPERATORS, NETWORK AND CABLE OPERATORS)**

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?

**Reply to 4.A.1:**

Please be informed that the electronic communications merchants provided the disclosure of communications data for the law enforcement authorities up to the implementation of the Directive 2006/24/EC.

In the result of the implementation of Directive 2006/24/EC it was determined in legislation of the Republic of Latvia that the electronic communications merchants have a duty to ensure the storage of data to be retained for 18 months (the Section 19(1) lit.11 of Electronic Communications Law). The period of storage of data for business purposes under Directive 2002/58/EC (the Section 6 lit. 2 of the Directive 2002/58/EC) is two years in Latvia. Wherewith the implementation of the Directive 2006/24/EC does not have the effect of requiring the electronic communications merchants 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.

**Reply to 4.A.2:**

The Section 71.1 (2) of Electronic Communications Law determines that an electronic communications merchant shall ensure the retention of retained data in such volume as they are acquired or processed in providing electronic communications services, as well as ensuring the protection thereof against accidental or unlawful destruction, loss or modification, or processing or disclosure not provided for in Electronic Communications Law. The electronic communications merchant does not have a duty to perform additional measures to acquire the data to be retained if in providing electronic communications a service, the technical equipment of the merchant doesn’t generate, process and register such data.

In accordance with Section 1 lit.8 of Electronic Communications Law *electronic communications merchant* – a merchant who ensures a public electronic communications network or provides electronic communications services.
Wherewith it means that all electronic communications merchants have a duty to save data.

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?

**Reply to 4.A.3:**

The retention of data in Latvia concerning fixed network telephony and mobile telephony is applied in practice since 16 June, 2007.

The retention of data in Latvia concerning Internet access, Internet e-mail and Internet telephony is applied in practice since 15 March, 2009.

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

4.A.4.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)?

**Reply to 4.A.5:**

We do not have information (also after consulting with association the electronic communications merchants) regarding necessary to implement any specific organisational measures and procedures. At the same time please be informed with the purpose to implement the requirement of the Directive 2006/24/EC the various administrative measures are implemented such as legislatively concerning procedures of issuing Data to be Retained to the law enforcement authorities.

In the some of the electronic communications merchants specific structural units deal with retaining, issuing, processing and deleting of Data to be Retain.
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]

Reply to 4.A.6: 
In the process of consulting with the electronic communications merchants we have received information that the electronic communications merchants have costs which have arisen fulfill obligations mentioned in point 4.A.4.a to 4.A.4.d (human resources, hard ware and soft ware). At the same time the precise costs which have arisen fulfill obligations from Directive are not indicated. They have indicated that it is not possible to quantify financial impacts of the necessary measures in so short time period.

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

Reply to 4.A.7: 
The Section 71.1 (2) of Electronic Communications Law does not foresee to collect the collateral data therefore the national legislation of Latvia does not include any reimbursement by national authorities.

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?

Reply to 4.A.8: 
The Section 19 (1) lit.4 of Electronic Communications Law determines the duty of electronic communications merchants to ensure the protection of user data including personal data in accordance with regulatory enactments.

The protection of personal data is provided by the Personal Data Protection Law.

Especially should be stressed the requirements of the protection of personal data if the processing of data is aided by the information systems. In this case the keeper of the information system shall observe the Regulations of the Cabinet of Ministers No.40 of 30 th January 2001 „The obligatory technical and organizing requirements of the protection of personal data”.

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 for a description of these problems.

Reply to 4.A.9: 
In accordance with the requirements of the Section 71.1 (3) of Electronic Communications Law an electronic communications merchant shall ensure the transfer of data to be retained on the basis of a request of pre-trial investigation
institutions, persons performing investigative field work, State security institutions, the Office of the Public Prosecutor and the courts in order to protect State and public security or to ensure the investigation of criminal offences, criminal prosecution and criminal court proceedings.

We do not have information that such kind of requests is carry out. In the process of consulting with the electronic communications merchants we have found out that till today they have not received request from authorities in another Member States.

4.A.10 Please provide information, differentiated by type of operator etc concerning the elements of section 1.A.1 of this questionnaire.

Reply to 4.A.10:
Statistics is attached in annex.

4.A.11 Which economic effect do providers observe

4.A.11.a on competition,

Reply to 4.A.11a:
We have not received confirmation that the implementation of requirements of the Directive 2006/24/EC evokes essentially the economic effect on competition.

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

Reply to 4.A.11b:

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.

Reply to 4.A.11c:
See question No. 4.A.6

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

Reply to 4.A.12.a:
Operators store data in the operators’ centres in the territory of the Republic of Latvia.

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?
Reply to 4.A.12.b:
Operators do not transfer retained data that are stored at centralised level to other 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.

Reply to 4.B.1:
In Latvia pre-paid SIM cards are used. Electronic Communications Law doesn’t determine the obligatory registration of users of pre-paid SIM cards.

In the consulting process by the electronic communications merchants we have found out that the electronic communications merchants have not been requested to identify users of pre-paid SIM cards.

Annex: Statistics of year 2008 on data retained pursuant to the directive 2006/24/EC on 1 sheet.
Statistics of year 2008 on data retained pursuant to the Directive 2006/24/EC

Country: LATVIA

### FIXED COMMUNICATION DATA

<table>
<thead>
<tr>
<th>Number of occasions where data provided to competent authorities during 12 month period</th>
<th>Age of data provided</th>
<th>Number of occasions where not possible to provide data</th>
</tr>
</thead>
<tbody>
<tr>
<td>698</td>
<td>0-3 month</td>
<td>44</td>
</tr>
<tr>
<td>213</td>
<td>3-6 month</td>
<td>26</td>
</tr>
<tr>
<td>167</td>
<td>6-9 month</td>
<td>9</td>
</tr>
<tr>
<td>193</td>
<td>9-12 month</td>
<td>1</td>
</tr>
<tr>
<td>104</td>
<td>12-15 month</td>
<td>3</td>
</tr>
<tr>
<td>137</td>
<td>15-18 month</td>
<td>7</td>
</tr>
</tbody>
</table>

### MOBILE COMMUNICATION DATA

<table>
<thead>
<tr>
<th>Number of occasions where data provided to competent authorities during 12 month period</th>
<th>Age of data provided</th>
<th>Number of occasions where not possible to provide data</th>
</tr>
</thead>
<tbody>
<tr>
<td>8928</td>
<td>0-3 month</td>
<td>419</td>
</tr>
<tr>
<td>2298</td>
<td>3-6 month</td>
<td>44</td>
</tr>
<tr>
<td>1085</td>
<td>6-9 month</td>
<td>25</td>
</tr>
<tr>
<td>746</td>
<td>9-12 month</td>
<td>26</td>
</tr>
<tr>
<td>394</td>
<td>12-15 month</td>
<td>16</td>
</tr>
<tr>
<td>257</td>
<td>15-18 month</td>
<td>0</td>
</tr>
</tbody>
</table>

### INTERNET COMMUNICATION DATA

There is impossible to specify the statistics of internet communication data classifying by internet access, internet telephony and internet e-mail, because of such classification is not required in accordance with the Electronic Communications Law and Regulations of Cabinet of ministers Nr.820 (December 4, 2007) that regulates the procedure of communication of the retained data to competent authorities and procedure of providing the statistics (that implements the requirements of Directive 2006/24/EC on the retention of electronic communication data).

<table>
<thead>
<tr>
<th>Number of occasions where data provided to competent authorities during 12 month period</th>
<th>Age of data provided</th>
<th>Number of occasions where not possible to provide data</th>
</tr>
</thead>
<tbody>
<tr>
<td>424</td>
<td>0-3 month</td>
<td>26</td>
</tr>
<tr>
<td>150</td>
<td>3-6 month</td>
<td>8</td>
</tr>
<tr>
<td>75</td>
<td>6-9 month</td>
<td>7</td>
</tr>
<tr>
<td>219</td>
<td>9-12 month</td>
<td>26</td>
</tr>
<tr>
<td>74</td>
<td>12-15 month</td>
<td>6</td>
</tr>
<tr>
<td>34</td>
<td>15-18 month</td>
<td>3</td>
</tr>
</tbody>
</table>

Evita Dzansukane, Data State Inspectorate of Latvia, +371 67223131