STATE DATA PROTECTION INSPECTORATE

To: Mr Wessel Dikker Hupkes  
European Commision  
DG JLS – F3  
e-mail address: wessel.dikker-hupkes@ec.europa.eu

CC: Ms Kelly Mathioudaki  
The Secretariat of the Article 29  
Data Protection Working Party  
e-mail address: Kalliopi.Mathioudaki-Kotsomyti@ec.europa.eu

Mr Tomas Žilinskas  
e-mail address: tomas.zilinskas@eurep.mfa.lt

Subject: Questionnaire for the Evaluation of Directive 2006/24/EC

Dear Mr Wessel Dikker Hupkes,

Please find attached the answers of the Republic of Lithuania to the Questionnaire for the Evaluation of the Directive 2006/24/EC.

Sincerely yours,

[Signature]

Dr. Algirdas Kunčinas  
Director of the State Data Protection Inspectorate of the Republic of Lithuania

Prepared by B. Jurgelevičienė, phone +370 5 262 0220

---

State Budgetary Institution  
A. Juncapavicius str. 6 / Slucko str. 2  
09310 Vilnius  
Tel. +370 5 279 1445  
Fax +370 5 261 9494  
E-mail ada@ada.lt

The data is collected and stored in the Register of Legal Persons  
Code 188607912
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.

I.A.1 Law enforcement issues

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

Total number of requests that are issued to obtain retained data from 15th March 2009 till 1st December 2009 is 79586. This number of requests is total number of requests issued by the operational entities for the purpose of the investigation of crimes and some requests for the purpose of the investigation of misdemeanours might be included.

According to the resolution of the Government No. 789 of 22nd July 2009 competent authorities shall provide the State Data Protection Inspectorate of the Republic of Lithuania (hereinafter – SDPI) with the statistical data for previous calendar year till 10th February every year. As a result, the SDPI, which is responsible for collection of such statistical data, asked figures indicated in the Directive, but received data might not by very precise.

There aren’t statistics on the outgoing requests from Lithuanian authorities for data listed in Directive 2006/24/EC from foreign countries. Approximately it could be about 70-90 per year.

I.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]

<table>
<thead>
<tr>
<th>Authority</th>
<th>Percentage of requests</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customs Criminal Service</td>
<td>12</td>
</tr>
<tr>
<td>Lithuanian Criminal Police Office</td>
<td>75</td>
</tr>
<tr>
<td>State Security Department</td>
<td>7</td>
</tr>
<tr>
<td>Special investigation service</td>
<td>1</td>
</tr>
<tr>
<td>Financial Crime Investigation Service</td>
<td>5</td>
</tr>
</tbody>
</table>

I.A.1.e 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 Article10 DRD. (Quantitative Reply)

It is not possible to provide exact statistical data on the time elapsed since the law enforcement inquiry and the data retention, since everything depends on the specific situation in each individual case, and the discovery of the criminal act itself. Average age of the data requested on fixed telephony events is about 7 months, and on mobile is about 3 months. So average age is about 5 months, but it shall be paid attention, that these numbers are only approximate.

I.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

Usually law enforcement authorities send requests to all communication operators and service providers and receive the answers from all of them. Requests are sent by e-mail, web interface or by paper form. The answers are provided by the same communication channel as the request was received. Requests and replies sent by e-mail and internet access are encrypted. Secure network is used in some cases. Secure https protocol is used for connection to web interface. Also leased lines (VPN technology) are used.
1. A. I.e Type of crimes

1. A. I.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

Criminal code and the Code of Criminal Procedures do not provide restrictions on the data acquisition depending on the type of offense.

Types of crime which national law authorise the acquisition, use and storage of retained data according to the provisions of the Directive are indicated in the Criminal Code of the Republic of Lithuania. According to the provisions of that Code all criminal acts shall be divided into crimes and misdemeanours. A crime shall be a dangerous act (act or omission) forbidden under this Code and punishable with a custodial sentence. A misdemeanour shall be a dangerous act (act or omission) forbidden under this Code which is punishable by a non-custodial sentence, with the exception of arrest.

Types of crime according to the provisions of Criminal Code of the Republic of Lithuania are as follows:
1. Crimes against humanity and war crimes
2. Crimes against the independence, territorial integrity and constitutional order of the State of Lithuania
3. Crimes against human life
4. Crimes against human health
5. Crimes endangering human health and life
6. Crimes against human liberty
7. Crimes against inviolability of a person’s private life
8. Crimes against intellectual and industrial property
9. Crimes against security of electronic data and information systems
10. Crimes against public security
11. Crimes against the activities of a civil servant or a person performing the function of public administration
12. Crimes against person’s voting rights and the procedure of elections of the President of the Republic of Lithuania, elections to the Seimas, the European Parliament and municipal councils or the procedure for conducting referendums

Types of the dangerous acts (act or omission) which might be crime and misdemeanours according to the provisions of Criminal Code of the Republic of Lithuania are as follows:
1. Crimes and misdemeanours against freedom of a person’s sexual self-determination and inviolability
2. Crimes and misdemeanours against a person’s dignity and honour
3. Crimes and misdemeanours against a child and a family
4. Crimes and misdemeanours against a person’s equal rights and freedom of conscience
5. Crimes and misdemeanours against a person’s social rights
6. Crimes and misdemeanours against property, property rights and property interests
7. Crimes and misdemeanours against the economy and business order
8. Crimes and misdemeanours against the financial system
9. Crimes and misdemeanours against civil services and public interest
10. Crimes and misdemeanours against justice
11. Crimes and misdemeanours relating to possession of weapons, ammunition, explosives, explosive or radioactive materials or military equipment
12. Crimes and misdemeanours relating to possession of narcotic or psychotropic, toxic or highly active substances
13. Crimes and misdemeanours against the environment and human health
14. Crimes and misdemeanours against traffic safety
15. Crimes and misdemeanours against public order
16. Crimes and misdemeanours against government order
17. Crimes and misdemeanours against government order relating to forgery of documents or measuring devices
18. Crimes and misdemeanours against morality
19. Crimes and misdemeanours against the memory of the deceased
20. Crimes and misdemeanours against national defence service

Also entities of the operational activities have right to use retained data according to the provisions of the Article 9 of the Law on Operational Activities of the Republic of Lithuania for an operational investigation purpose. According to the Law on Operational Activities traffic and identification of users’ data also were used before transposing the Directive. An operational investigation shall be conducted, when:

1) characteristics of a criminal act have not been established, but information is available about a particularly serious or serious crime being prepared, being committed or having been committed or less serious crimes provided in the Criminal Code of the Republic of Lithuania or about a person preparing, committing or having committed a crime;
2) information is available about the activities of the special services of other states;
3) the suspect, the accused or the convicted person goes into hiding;
4) a person is reported missing;
5) protection of persons against criminal influence is being implemented;
6) protection of state secrets is being implemented;
7) information is available about the acts posing a threat to the constitutional system of the State, independence and economic security thereof, ensuring of the defence power of the State or other interests of importance to national security.

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)

Statistics about average age of the data due to unjustifiably high cost of working time are collected only in the Lithuanian Criminal Police Office and only of requests for fixed network and mobile network telephony data. Average age of the data is 101,6 day. Statistics by some of crimes:

<table>
<thead>
<tr>
<th>Type of Crime</th>
<th>Average age of the data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Production, storage or handling of counterfeit currency</td>
<td>159</td>
</tr>
<tr>
<td>Unlawful deprivation of liberty</td>
<td>158</td>
</tr>
<tr>
<td>Cyber crime</td>
<td>154</td>
</tr>
<tr>
<td>Criminal association</td>
<td>136</td>
</tr>
<tr>
<td>Human trafficking</td>
<td>133</td>
</tr>
<tr>
<td>Pornography</td>
<td>125</td>
</tr>
<tr>
<td>Falsification of the documents</td>
<td>123</td>
</tr>
<tr>
<td>Swindling</td>
<td>119</td>
</tr>
<tr>
<td>Search</td>
<td>114</td>
</tr>
<tr>
<td>Abuse of authority</td>
<td>111</td>
</tr>
<tr>
<td>Swindling in grand dimension</td>
<td>111</td>
</tr>
<tr>
<td>Premeditated severe health impairment</td>
<td>109</td>
</tr>
<tr>
<td>Murder</td>
<td>108</td>
</tr>
<tr>
<td>Extortion of property</td>
<td>106</td>
</tr>
<tr>
<td>Smuggling</td>
<td>106</td>
</tr>
<tr>
<td>Unauthorised migration</td>
<td>103</td>
</tr>
<tr>
<td>Threat, terrorism</td>
<td>100</td>
</tr>
<tr>
<td>Arms, ammunition</td>
<td>97</td>
</tr>
<tr>
<td>Drugs</td>
<td>93</td>
</tr>
</tbody>
</table>
Self-Willed Conduct 88
Malignant hooliganism 88
Theft of cars 86
White washing (Money laundering) 83
Rape 82
Non-Severe Health Impairment 73
Destruction of or Damage to Property 70
Murderous attempt 69
Acceptance of bribe 65
Terrorism 62
Robberies 61
Thefts 58

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

National law allows receiving traffic data from communication operators and service providers for investigation and detection of dangerous acts indicated in the Criminal Code and fulfilling obligations according to the provisions of the Law on Operational Activities, for example public and secret activity related to the intelligent services. All public and secret activities of the intelligent services shall be governed by the principles of lawfulness, ensuring human and citizens’ rights and freedoms, protection of the public interest, conspiracy, confidentiality and etc.

Basics of the operational investigation according to the Article 9 of the Law on Operational Activities are as follows:

An operational investigation shall be conducted, when:

1) characteristics of a criminal act have not been established, but information is available about a particularly serious or serious crime being prepared, being committed or having been committed or less serious crimes provided for in Article 131 (infanticide), paragraph 2 of Article 145 (Threatening to murder or cause a severe health impairment to a person or terrorisation of a person), paragraphs 2 and 3 of Article 146 (unlawful deprivation of liberty), paragraph 1 of Article 150 (sexual assault), paragraph 2 of Article 151 (sexual abuse), Article 162 (use of a child for pornography), paragraph 2 of Article 178 (theft), paragraph 1 of Article 180 (robbery), paragraph 1 of Article 181 (extortion of property), paragraph 2 of Article 187 (destruction of or damage to property), paragraph 2 of Article 189 (acquisition or handling of the property obtained by criminal means), paragraph 2 of Article 198 (unlawful interception and use of electronic data), paragraph 1 of Article 213 (production, storage or handling of counterfeit currency or securities), Articles 214 and 215 (production of a counterfeit electronic means of payment, forgery of a genuine electronic means of payment or unlawful possession of an electronic means of payment or data thereof and unlawful use of an electronic means of payment or data thereof), paragraph 2 of Article 225 (bribery), paragraph 2 of Article 227 (graft), paragraph 2 of Article 228 (abuse), Article 240 (freeing a prisoner), paragraph 1 of Article 253 (unauthorised possession of firearms, ammunition, explosives or explosive materials), paragraph 1 of Article 256 (unlawful possession of nuclear or radioactive materials or other sources of ionising radiation), paragraph 2 of Article 300 (forgery of a document or possession of a forged document), paragraph 2 of Article 301 (forgery of a seal, stamp or form), paragraph 2 of Article 302 (seizure of a seal, stamp or document or use of the seized seal, stamp or document) and paragraphs 1 and 2 of Article 307 (gaining profit from another person’s prostitution) of the Criminal Code of the Republic of Lithuania or about a person preparing, committing or having committed a crime;

2) information is available about the activities of the special services of other states;
3) the suspect, the accused or the convicted person goes into hiding;
4) a person is reported missing;
5) protection of persons against criminal influence is being implemented;
6) protection of state secrets is being implemented;
7) information is available about the acts posing a threat to the constitutional system of the State, independence and economic security thereof, ensuring of the defence power of the State or other interests of importance to national security.

Entities of the operational activities have right to receive an information related to the intelligent services about past telecommunication connections only having a reasoned court ruling.

In some cases receiving of the retained data indicated in the Directive is limited by the Constitution of the Republic of Lithuania, Criminal Code of the Republic of Lithuania and the Law on Operational Activities of the Republic of Lithuania.

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.

The Article 5 of the Directive was fully transposed into national law as regards the scope of the data and entered into force on 16th March 2009. However analyzing systemically with the Article 5 of the Directive after amending it to the national law some service providers are obliged to process and retain data they had not been processing and retaining before. For example mobile service providers who were not retaining data on unsuccessful calls attempts.

Also some of the mobile service providers still do not collect and provide the following data:
- data necessary for place identification of mobile phones, notation of the place (Cell ID) at the beginning of the connection of the mobile service (“Bité”, “Tele2”);
- about the connection equipment used for mobile services (IMEI) when SMS are sent and received (short text messages)- “Tele2”;
- about unsuccessful calls attempts (“Bité”).

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.

All data indicated in Article 5 of the Directive are necessary.

It would be useful to supplement the list of data of mobile services indicated in Article 5 of the Directive by following data:
- “Switch on” and “switch off” time (manual, when energy is lost, when the device falls into the water) data and time, IMEI, IMSI, notation of the place (Cell ID), in which that event happened;
- Establishment of the geographical location of the telephone set number which operates in the operator’s network in real time.
These data are necessary for the competent authority fulfilling search of the persons who are kidnapped or in a helpless state, or who have performed or are going to perform an act of terrorism or other crime.

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

I.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 most common types of requests:
1. Detailed list by number
2. Detailed list by IMEI MIN / MAX MSISDN
3. Owner search IMSI
4. Detailed list by OMSI MIN / MAX MSISDN
5. Detailed list by number of callee
6. Detailed list by number B who called this number
7. Detailed list by MSISDN MIN / MAX IMEI
8. Detailed list by MSISDN MIN / MAX IMSI
9. Data about the subscriber (person or company)
10. Owner search by IMSI
11. Owner search by SIM
12. Information about pre-paid cards (Bitė Lietuva)
13. History of subcribed number (Omnitel)
14. PIN and PUK codes determination
15. (CELL)- detailed connections by location labels (Cell ID) number
16. Refills of the pre-paid card user’s account

Parameters of request: object (phone, IMEI, IMSI, Cell ID, etc.) number, type of information (dependence, call Fact Sheet), data period (from-to date), the competent authorities requests a unique number (ID number of the query sequence).

I.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.

Lithuania wants to establish a centralized electronic system of the data of past events and participants for the use to all competent authorities. In order to avoid compatibility problems with the data exchange of information between national and international institutional systems, it will be created in accordance with the ETSI (European Telecommunications Standards Institute) standards. What is more, law enforcement authorities and service providers have signed agreements on acquisition and disclosure of communications data.

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 communications data enable the public authority to specify the time period within which data must be disclosed, as referred to in the Directive as “without undue delay”. If so:

1. A.1.h.1 Please provide examples of time frames enforceable within the context of national legislation or by service level agreements between competent authorities and communication providers.
Terms for provision of traffic data are not regulated in national legal acts or contracts.

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

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

It is often important to have rapid response according to various types of data or in individual cases for the competent authority. Service providers provide data according to the order of received requests or according to the type of data to be provided, regardless of the urgency of execution.

1.A.1.i Reimbursement of costs

1.A.1.i.1 Does your country reimburse CAP EX\textsuperscript{4} and/or OPEX\textsuperscript{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.

In a case if law enforcement authorities ask service providers to retain traffic data for more than 6 months (in this case traffic data could be retained for not more than 6 months additionally) service providers have the right to reimbursement of costs.

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.

It is not determined. The costs of the service providers depend on the form of inquiry: paper or electronic form. Pre-trial investigation agencies, prosecution, courts are inquiring by paper form quite often. National legislation does not provide reimbursement for the provision of documents or data in paper form (the cost of staff time, printing, postage costs). As a result, service providers are interested to provide extensive fixed and mobile communications data electronically. The competent authorities fund operating costs of safety nets and software interface given by service providers (to receive the retained data) at their own expenses.

The cost of inquiries and the provision of data by e-mail are not reimbursed for the service providers.

We have no data on costs and reimbursement of them of the provision of Internet connection data.

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 use of retained data do assist in investigation of crimes and in some cases, such as investigation of criminal acts committed in cyberspace, investigation without retained data (for example a dynamic IP address at a specific time dependence) is not possible at all. Since in the Law on Electronic Communication of the Republic of Lithuania is established the provision to preserve data generated for 6 months from the beginning of e-flow, it is common events, especially when carried out international legal assistance requests (from foreign countries it is often that inquiries are received for criminal acts committed in 2007 or later), when due to the passage of time data on the e-flow is no longer available. In view of it the police hold the opinion that the Directive should clearly establish that generated data shall be kept for 24 months. This will strengthen international
cooperation in law enforcement while investigating offenses committed in cyberspace, as the data on e-flow events are usually the only way to investigate such offenses.

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

There is no such calculation.

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

The price and performance ratio of the data stored can be improved while introducing a unified centre of electronic data of past events and their participants, thus removing the cost of hiring the necessary communication channels from each operational entity to operators of e-communication (the channels of communication from each operational entity will be needed only until the centre), as well the part of the cost required to collect statistical information and provide the European Commission could be removed, whereas the current situation to provide statistical information requires a lot of time and human resources.

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

Overall, during the year 2008 are send 675 legal assistance requests (353 through Prosecution service of the Republic of Lithuania and 322 through the districts), from foreign countries received 552 (312 through Prosecution service of the Republic of Lithuania and 240 through districts) requests. Statistical accounting of the outgoing and incoming requests related to Directive 2006/24/EC is not carried out avoiding significant additional work time and other resources. However, it can be assumed that such requests constitute about 10 percent of all requests.

1.A.2.a.4 what is the ratio between national and transnational requests (total number of transnational requests)? Quantitative Reply

There is no statistical data about requests sent by institutions of Lithuania as regards the data indicated in the Directive 2006/24/EC and replies collected. Approximately it could be about 70-90 times per year.

In the absence of statistical data there is no possibility to compare requests of national and international level on the data listed in Directive 2006/24/EC.

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.J)? What are the elements (for instance: type of procedure) that determine the length of the procedure Quantitative elements
The time lag records between the request and the response are not counted for clearly excessive costs. However, usually a request for legal assistance in a criminal case consists of a number of issues, of which only part concerns the data listed in Directive 2006/24/EC. Due to that the answer to the requesting State is usually sent after all the required actions are completed. However, in all cases, the enforcement processes terms in requested country depends on a number of competent bodies to which the application is being referred, to the time necessary for translations (if necessary) into the state language, how long it takes to authorize data collection at a prosecutor or pre-trial judge, how long it takes technically to search data and make a backup copies, what translations are made and procedural documents drawn up, number of competent bodies participating in preparation and translation into the language required of response text, the manner in which it is sent and etc. organizational factors.

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/

The same as in question 1.A.2.b.1.

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

Establishment of the central point that would receive inquiries, collect data received from service providers, issue outgoing requests and conduct communication with foreign countries could help to reduce the time for answering to incoming requests.

Also these measures could be helpful:
- standardization of collected data;
- use of the special equipment for online connections when the competent authority is executing data collection;
- automatic measures for data processing, dedicated for composing electronic inquiries. These measures should be used for sending of these inquiries to the service providers, registration of received responses, storage and distribution to competent institutions and divisions.

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?

Prosecutors are authorised to make the decision to issue a transnational request for retained data and Central Office of the Prosecution Service or Prosecution Services of the districts are authorised to send collected information. Such type data shall be collected only employing measures of compulsion applied by the State, indicated in the Code of Criminal Procedure which is imposed by a court’s judgment. In criminal matters any answer to the transnational request for the data indicated in the Directive 2006/24/EC would not be sent without Prosecutors’ knowledge.

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.

There is no one such central point.
Pre-trial investigation institutions of the Republic of Lithuania and regional Prosecution Services should send requests for legal assistance in criminal cases as regards data indicated in the Directive 2006/24/EC through Central Office of the Prosecution Service or 5 Prosecution Services of the districts, depending on what international conventions on legal assistance the requested state has ratified and what notifications or exemptions have been done.

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?
All costs related to the international requests are covered by competent institution (receiving party). There is no intention to share them.

1. A. 2. f. Language

1. A. 2. / 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.

Lithuania has made such statements and reservations on the language of legal assistance requests: the Council of Europe 1959 Convention on Mutual Assistance in Criminal Matters - requests shall be in the one of official languages of the European Council, in the 2000 MS Convention on Mutual Assistance in Criminal Matters - the language is vague.

Lithuania has no any centralised body responsible for translations in national or foreign languages.

1. A. 2. / 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?

Depending on the language of the foreign request, the prosecution service or the translation units (in which is limited number of languages, especially in the territorial district prosecution services) makes translation of the documents to the Lithuanian or contact the official translation agency.

Lithuania has no any centralised body responsible for translations in national or foreign languages.

1. A. 2. g. Data security

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

Controllers of information systems in public institutions have to agree with the Ministry of Interior and to approve these documents: resolutions, procedures for secure processing of electronic information, plans for continuity management of activity of information system, rules for administration of information system users.

The State Data Protection Inspectorate has the right to perform audits concerning personal data protection.

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?

There is no any appointed body which would be in charge with general tasks of the implementation of the Directive (clarification of the applicable law, specifying which data should be retained, on standardization of data inter exchange, evaluation of operator’s costs).

The State Data Protection Inspectorate is responsible for providing the European Commission with statistics on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or a public communications network according to the Article 10 of the Directive 2006/24/EC.
Lithuania is planning to establish a working group that would deal with the questions concerning application of the Directive.

1A3a2 When did/will the respective authorities start to be operational for these tasks?

The State Data Protection Inspectorate was found before the Directive 2006/24/EC was implemented. According to the Law on Legal Protection of Personal Data the State Data Protection Inspectorate has supervision powers towards all data controllers, including law enforcement authorities, except when personal data are processed for the purposes of State security or defence. Competencies regarding statistics on the retention of traffic data were supplemented by the Resolution of the Government No. 789 of 22nd July 2009.

1A3a3 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?

To have in mind that amendments of the Law on Electronic Communications entered into force on 15th March 2009 and Resolution of the Government No. 789 of 22nd July 2009 entered into force on 15th September 2009 there is no practice how to deal with data retention issues.

The State Data Protection Inspectorate started the inspection of 4 communications operators to check how the process is going and how data subjects’ rights are protected.

1A3a4 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/

There is no information at the moment. The breaches of the Law on Copy Right are not treated as serious crime according to the Lithuanian law.

1A3a5 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/

To this moment any authority mentioned under this section do not engage in cross-border co-operation relating to the Directive. However the SDPI participated in a few conferences where issues related to the privacy protection implementing Directive 2006/24/EC were discussed. Also SDPI is active member of the Working Party on Data Protection of Article 29 of Directive 95/46/EC which is dealing on data protection problems as regards data retention.

1A3a6 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/

Above mentioned competencies by national legislation are granted to the Communication Regulatory Authority but the Communications Regulatory Authority (as well as any other authority) does not gather any data concerning the impact of the transposed Data Retention Directive regulations on competition in electronic communication market.

1A3a7 Centralised storage of data by Service providers
Does your country have problems (e.g. time to obtain an answer, quality of the reply) to obtain retained data that are stored by service providers outside of your country. Please provide details of problems you may have experienced and means deployed to redress these problems. [can entail Quantitative elements]

Service providers are obligated to collect, retain and provide traffic data by the Law on the Electronic Communications of the Republic of Lithuania does not matter there they store such data, so by this moment there is no information on problems to obtain data stored outside Lithuania.

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.

The national law does not provide any measures in order to ensure the identification of users of prepaid SIM cards. Also Lithuania has not deployed any measures listed in the question above. The identification is basically done on voluntary basis. Law enforcement authorities emphasize that because of that reason investigation of crimes becomes unreasonably long and sometimes even unsuccessful. The registration of traffic data of prepaid SIM cards is started from the moment when the first outgoing call is done. Telecommunications providers are free to set terms for how long prepaid SIM cards remain valid. For example, one telecommunications provider has determined that outgoing calls could be done 100 days after supplementing the account of prepaid SIM card. Incoming calls could be received for 200 days additionally.

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.

Lithuania has not deployed any measures listed in the question above.

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/.

Lithuania has not deployed any measures listed in the question above.

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

Lithuania has not deployed any measures listed in the question above.

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

Lithuania has not deployed any measures listed in the question above.

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

Lithuania has not deployed any measures listed in the question above.

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?

According to law enforcement authorities, the Directive 2006/24/EC could be amended as follows:

-it would be positive if data retention time should be the same in all Member-States (12 months) or if it is justifiable even for longer period.
-an obligation to register the owners of pre-paid SIM cards in order to ensure the identification of users to be introduced.
-to authorise the acquisition and use of retained data for all types of crimes and misdemeanours, not only for serious ones.

According to The State Data Protection Inspectorate, the retention period should be 6 months.

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?

There is no information on such trainings.

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?

Lithuania has not deployed any measures listed in the question above.

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

Lithuania has not deployed any measures listed in the question above.

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]

Lithuania has not deployed any measures listed in the question above.

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?

Lithuania has not deployed any measures listed in the question above.
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?

It would be useful to organize European wide informational campaign in order to explain in more detail that under the Directive there is retained only traffic data, but not the content of emails, conversations and etc. A biggest part of negative reaction from society was based on confidence that when the Directive will come into force, operators will retain and law enforcement authorities will obtain retained data about content of communication.

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.

The national law does not provide any measures in order to ensure the identification of users of prepaid SIM cards. Also Lithuania has not deployed any measures to increase the traceability of users of communication devices.

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.

The Directive 95/46/EC is transposed into Lithuanian law by the Law on Legal Protection of Personal Data (LLPPD). According to the paragraph 1 of the Article 36 of the LLPPD the implementation of this Law, with the exception of Article 8, shall be supervised and monitored by the State Data Protection Inspectorate (SDPI).

The Directives 2002/58/EC and 2006/24/EC are transposed into Lithuanian law by the Law on Electronic Communications (LEC). According to the subparagraph 1 of the paragraph 1 of the Article 9 of the LEC the Communications Regulatory Authority (CRA) shall exercise control over, supervision of and implementation of the provisions of this Law and the legal acts implementing it, except where such control, supervision and implementation fall within the scope of competence of other state institutions as defined by this Law. According to the paragraph 1 of the Article 8 of the LEC, the CRA has the objective of developing effective competition in the field of electronic communications, efficient use of electronic communications resources and ensured protection of the rights of consumers of electronic communications services. Whereas the SDPI is responsible for the supervision of the implementation of provisions of Chapter 9 of this Law (Processing of Personal Data and Protection of Privacy), except for paragraph 5 of Article 61, paragraph 7 of Article 64 and paragraph 2 of Article 68 (paragraph 5 of the Article 12 of the Law on Electronic Communications).

Also the SDPI is responsible for providing the European Commission with statistics on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or a public communications network according to the Article 10 of the Directive 2006/24/EC.

3.A.1 Do authorities have investigative powers vis-a-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.

Yes, they do. The SDPI has not received any complaints concerning retention of data according to the Directive 2006/24/EC.

The SDPI is performing preventive audits at 4 telecommunication companies working in Lithuania as it was agreed by the Working Party on Data Protection of Article 29 of Directive 95/46/EC currently.

3.A.2 Do authorities have investigative powers vis-a-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.

Yes, they do. The SDPI has not received any complaints concerning retention of data according to the Directive 2006/24/EC.

The SDPI is performing preventive audits at 4 telecommunication companies working in Lithuania as it was agreed by the Working Party on Data Protection of Article 29 of Directive 95/46/EC currently.

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]
Yes, they do. The SDPI is performing an audit at 4 telecommunication companies working in Lithuania as it was agreed by the Working Party on Data Protection of Article 29 of Directive 95/46/EC currently. The official outcome of the proceedings is not ready yet, but preliminary we could inform that the SDPI has not found out any breaches of national legal acts regulating data protection. All above mentioned telecommunication companies will be provided with recommendations how they could improve processing of traffic 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]

The SDPI has not identified problems with the practical implementation of the Directive yet.

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

The SDPI is performing an audit at 4 telecommunication companies. Three of them reported that traffic data are stored in Lithuania. One company pointed out that traffic data is stored in other EEA countries. The SDPI has not had more experience on this issue.

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?

There is not any case law with regard to the implementation or use of the Data Retention Directive or concerning the use of retained data within criminal investigations.

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]

As much as the State Data Protection Inspectorate has experienced there is no direct possibility to identify users of mobile phone lines, opened with pre-paid SIM cards. The national law does not provide any measures in order to ensure the identification of users of prepaid SIM cards. Also Lithuania has not deployed any measures to increase the traceability of users of communication devices.
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?

The Law on Electronic Communications obliges communications operators and service providers to retain data for the same period which they are doing for business purposes – 6 months (the same period for Directives 2002/58/EC and 2006/24/EC). In addition law enforcement authorities may ask service providers to retain traffic data for up to 6 months additionally.

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.

National law is applicable to all communications operators and service providers, thus the obligation to retain traffic data is applicable to all without any 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?

The amendments of the Law on Electronic Communications transposing the Directive 2006/24/EC entered into force since 16 March 2009. The obligation to retain traffic data is applicable to all communications operators and service providers without any differentiation.

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,

Network operators’ providing public communication services investments were done before the adoption of the Directive, so additional investments were not needed. Information on service providers’ investments is not available.

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

Security of created databases is an integral requirement for these systems and there is no data on potential investment difference (in a case if there were no safety requirements).

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

The term "undue delay" was not specified in the Lithuanian legislation. Transposing the Directive into national law, it was agreed that the provision does not affect the update time of data bases, but concerns only the terms to reply to the AOC. However the time limits within which the query could be executed according to technical and organizational means should not be significantly (intentionally) exceeded.

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.
Network operators’ providing public communication services investments were done before the adoption of the Directive, but additional requirements for saving data of unanswered calls, postal data required additional investment. It is a relatively small investment for network operators providing public communication services. There is no information on service providers.

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)?

Network operators’ providing public communication services perform the data processing in good will and in accordance with bilateral agreements with the AOC.

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]

Network operators’ providing public communication services investments were done before the adoption of the Directive, so additional investments were not needed. Information on service providers’ investments is not available. So there is no possibility to quantify financial impacts this measures.

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

In a case if law enforcement authorities ask communications operators and service providers to retain traffic data for more than 6 months (in this case traffic data could be retained for not more than 6 months additionally) they have the right to reimbursement of costs. In reality, this right is not used and any costs are not reimbursed yet.

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?

Lithuanian major fixed network operator agrees that there is no ambiguity on this issue.

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.

No, they have not.

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

There is no such information available.

4.A.11 Which economic effect do providers observe

4.A.11.a on competition,

Network operators providing public communication services did not feel significant impact.

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

Substantial investments were not necessary for network operators providing public communication services.
4.A.11.e retail tariffs? Please provide quantitative information, and where such is not possible, qualitative indicators to allow assessment of the economic effect.

Network operators providing public communication services, did not raise prices for consumers due to the implementation of the Directive, because of the significant competition and their aim to have the biggest as possible penetration in the market.

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

One network operator stores traffic data in Lithuania, Latvia, Estonia and Sweden.

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?

Operators do not have right to transfer data under the Data Retention Directive. Whoever the retained data could be disclosed to other countries according to legal assistance applications.

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

The national law does not provide any measures in order to ensure the identification of users of prepaid SIM cards. Also Lithuanian communications operators and service providers has not deployed any measures to ensure the traceability of users of communication services and 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.

According to national law there is no obligation to the service providers to identify the pre-paid SIM cards users. Due to that and significant competition and aim to have the biggest as possible penetration in the market pre-paid SIM cards are realized without any identification of users, so there is no possibility to the service providers to identify such users. This means that law enforcement authorities in aim to identify user of the pre-paid SIM card need to investigate all connections from and to such a card, refills of the account, registration to the base and etc.